

# **Assessment of Savannah River Site's Software Quality Assurance Processes for Safety System Software and Firmware for Safety Systems**

**(SQAIP 4.2.3.3)**

**On-site Assessment 2/18/04 – 2/19/04**

3/18/2004

FSS-TQS-2004-00001

## Signature Page

Gregg Nelson	<u>Gregg Nelson (KM)</u> Signature	<u>3-25-04</u> Date
Chip Lagdon	<u>Chip Lagdon (KM)</u> Signature	<u>3-18-04</u> Date
Keith Morrell	<u>Keith Morrell</u> Signature	<u>3-18-04</u> Date
Vince Grosso	<u>Vince J. Grosso</u> Signature	<u>3-18-04</u> Date
Elaine Doolittle	<u>Elaine Doolittle</u> Signature	<u>3-22-04</u> Date
Dennis Adams	<u>Dennis Adams (KM)</u> Signature	<u>3-18-04</u> Date
Dan Zweifel	<u>Dan Zweifel</u> Signature	<u>3-18-04</u> Date
<i>(Bill was not able to attend on Feb 18. He has reviewed and concurs with this report)</i>		
Bill Rowland	<u>Bill Rowland</u> Signature	<u>3/23/04</u> Date

(In the event all team member signatures cannot be obtained due to logistical considerations, the assessment team leader should obtain members' concurrence and sign for them.)

## Signature Page

# Table of Contents

1.0	Introduction.....	2
1.1	Reason for Assessment .....	2
1.2	Background .....	2
1.3	Savannah River Site .....	2
1.4	Summary of approach: .....	2
2.0	Summary of Assessment .....	2
2.1	Highlights:.....	2
3.0	Lessons Learned.....	2
3.1	Positive Lessons / SRS SQA.....	2
3.2	Noted Items / WSRC Actions:.....	2
4.0	Detailed Results .....	2
4.1	Software Quality Assurance Program.....	2
	Criteria Met: YES .....	2
4.2	Software Requirement Description.....	2
	Criteria Met: YES .....	2
4.3	Software Design Description.....	2
	Criteria Met: YES .....	2
4.4	Software Testing, Acceptance and Turnover (SRS terminology) .....	2
	Criteria Met: YES .....	2
4.5	Software User Documentation.....	2
	Criteria Met: YES .....	2
4.6	Software Configuration Management .....	2
	Criteria Met: YES .....	2
4.7	Software Quality Assurance.....	2
	Criteria Met: YES .....	2
4.8	Software Procurement.....	2
	Criteria Met: YES .....	2
4.9	Software Problem Reporting and Corrective Action.....	2
	Criteria Met: YES .....	2
5.0	Attachments .....	2
5.1	Background information on Assessment Team .....	2
5.2	Lines of Inquiry Summary.....	2
5.3	Assessments Documents Reviewed List.....	2
5.4	WSRC SQA Procedures List .....	2
5.5	Glossary (U) Revision No. 35 January 30, 2004 .....	2

# 1.0 Introduction

---

## 1.1 Reason for Assessment

---

This assessment is a deliverable for a commitment of the U. S. Department of Energy Implementation Plan for Defense Nuclear Facilities Safety Board Recommendation 2002-1 Quality Assurance for Safety Software at Department of Energy Defense Nuclear Facilities.

**Commitment 4.2.3** Complete the identification, selection, and assessment of safety system software and firmware at defense nuclear facilities.

## 1.2 Background

---

The Defense Nuclear Facilities Safety Board (Board) issued Recommendation 2002-1, Quality Assurance for Safety-Related Software, on September 23, 2002. In that Recommendation, the Board noted its concerns regarding the quality of the software used to analyze and guide safety related decisions, the quality of the software used to design or develop safety-related controls, and the proficiency of personnel using the software. In addition, the Board noted that software performing safety-related functions in distributed control systems, supervisory control and data acquisition systems, and programmable logic controllers (PLCs) requires appropriate quality assurance controls to provide adequate protection for the public, the workers, and the environment.

## 1.3 Savannah River Site

---

The Savannah River Site (SRS) is a Department of Energy (DOE) facility that provides products and services essential to achieving the DOE's goals including:

- Nuclear Weapons Stockpile Stewardship
- Nuclear Materials Stewardship
- Environmental Stewardship

SRS occupies approximately 310 square miles, (about the size of the area inside the Washington, D.C. beltway) and is located 12 miles south of Aiken, South Carolina on the Savannah River which forms the boundary between South Carolina and Georgia. Augusta, Georgia is about 25 miles northwest of the site. Established in 1950 by the Atomic Energy Commission, SRS has been involved in the production of tritium and plutonium in support of the nation's nuclear stockpile.

SRS supports missions for both DOE National Nuclear Security Administration (NNSA) and DOE-Environmental Management (DOE-EM) organizations. The SRS Software Quality Assurance (SQA) program has one set of processes and procedures that apply for both NNSA and DOE-EM. This software at SRS is used for both NNSA and DOE-EM work. This assessment action was a combined effort of the NNSA Savannah River Site Office (NNSA-SRSO), DOE-EM, DOE-HQ, and Westinghouse Savannah River Company (WSRC).

---

## 1.4 Summary of approach:

---

The assessment team established a schedule to complete the assessment of the processes in place to ensure that safety system software has the high level of quality needed to provide adequate protection for the public, the workers, and the environment at defense nuclear facilities. Safety system software and firmware used in instrumentation or process control for nuclear facilities. To assess its adequacy the following steps were completed.

- Identify Assessment team members
- Develop Lines of Inquiry (LOI) for Assessment
- Identify Software for Assessments
- Conduct assessments per schedule
  - Contact owner of system to be assessed
  - Meet and collect documentation
  - Analyze documentation per LOI
  - Interview owner, users, and support personnel for system
  - Generate and Review Assessment reports
  - Take actions as required

This assessment reviewed the SRS Software Quality Assurance (SQA) processes and how they are implemented for Safety Systems Software and Firmware. The team reviewed Tritium Extraction Facility (TEF) Worker Protection System (WPS) and the Tritium Facility Modernization and Consolidation Project (TCON) Worker Protection System.

The LOI (attachment 5.2) was developed focusing on these major topical areas:

- QA / SQA Program & Processes
- Total Lifecycle of Software
- Requirements
- Design and Development
- Testing, Acceptance, and Turnover (others define as part of V & V)
- Operations and Maintenance
- Documentation
- Other related areas (procurement, security, past assessments, etc)

---

## 2.0 Summary of Assessment

---

An overview presentation of the SRS Quality Assurance (QA) program and the SRS Software Quality Assurance (SQA) program was given on February 18 to provide all team members an understanding of the SRS SQA foundation. On February 19 additional details of the SRS SQA process for handling Design and Analysis software was presented. This made it clear that SRS has one SQA program that addresses all software, including Safety System Software and Firmware.

The assessment team found that the SRS SQA program met the assessment criteria. A couple of items were noted during the assessment and required additional research. The

items and the SRS follow-up is included in the next section of this report, 3.0 Lessons Learned. The SRS SQA program and documents reviewed clearly show that the SRS SQA program includes Safety System Software and Firmware. The program as executed will maintain reliability of the software over its life cycle.

Assessment highlights are provided below, details are provided in the 4.0 Detail Results, and via the following attachments: 5.2 Lines of Inquiry (LOI) summary, 5.4 WSRC SQA Procedures List and the 5.3 Assessments Documents Reviewed List.

Based on these results and past assessments no additional assessments will be conducted at SRS for Safety System Software and Firmware for the SQAIP 4.2.3 action in response to DNFSB 2002-1. It is recommended that SRS continues its current SQA program, making improvements and conducting periodic assessments as needed. System availability and other process based metrics have been and will be applied where applicable.

---

## **2.1 Highlights:**

---

### ***SRS SQA Program***

(Was developed / based on the following)

- Based on Industry Standards, Federal Regulations, DOE Orders and best practices
- Integrated in QA program and Safety Management (QA / ISMS)
- Tracks contractual commitments related to QA / SQA via S/RID system
- Covers all software, including Safety System Software and Firmware
- Software Classification process / Safety criteria applied
- Graded approach
- Covers entire lifecycle from conception through retirement
- Connected to Procurement process
- Applies to developed , procured , and acquired software
- A Software Quality Assurance Plan (SQAP) is required for Safety Software
- Recent assessments and reviews have been very positive

### ***TEF WPS and TCON Software***

- Software Quality Assurance Plans
- Requirements Documents
- Diagrams used to clarify requirements
- Review and Approval of documents
- Change Control / Configuration Management
- Tracked changes through process
- Problem Reporting and Correction action
- Lessons learned are applied from existing systems
- Requirements are clearly traceable through testing
- Factory and Site acceptance testing
- Training is coordinated
- Independent review process

## 3.0 Lessons Learned.

---

### 3.1 Positive Lessons / SRS SQA

---

The following is a list of the positive aspects of the SRS SQA program assessed.

- SQA program is part of QA program
- One QA / SQA program for the Site
- All software including Safety Software covered
- Software classification process
- Graded approach
- Based on proven standards and government rules / orders / guidance
- Covers entire lifecycle (conception through retirement)
- Covers developed procured or acquired software.
- Involvement with standards and industry organizations provides benefits
- Configuration Management / Change Control
- Testing process
- Independent Review
- Training provided
- Lessons learned are applied
- Problem Reporting and Correction process
- Defined roles and responsibilities
- Review and approval required
- Documentation requirements
- Procurement and Security requirements are connected
- Error notification process

---

### 3.2 Noted Items / WSRC Actions:

---

1. Some problems with the site acceptance test in that some test data sheets were not signed, dated, and some of the columns were not filled out. If these particular columns are not applicable, they should be marked as "NA". Also many of the page numbers on the test data sheets were not legible. On some test data sheets the test was marked as "passed" while on others there was no clear indication that the equipment passed the test.

#### ***WSRC Response / Actions to Improve (Accepted)***

In an effort to minimize the size of the Site Acceptance Test (SAT) document during the review and approval process, only blank data sheets for each type of I/O module were included (i.e. reference the text for section 8.0 on page 22 of 32 of B-TPR-H-00116, "Data sheets for each module type are on pages 23 through 32. Test personnel are to photocopy data sheets as needed to cover all of the tested components"). This accounts for the blank sheets/columns and reduced the size of the TEF WPS SAT document by nearly one hundred pages. However, it does create the situation where multiple pages

within the test record have the same page number. At the time of the testing, test personnel attempted to address this problem by lining through the repeating page numbers and writing in new numbers by hand. In hindsight, this practice creates some confusion. In future testing, we will include specific data sheets in the SAT document for each tested component despite the increase in size to the test document.

2. There was a requirement that input to output of the controller be within 2 seconds. The documentation say that this requirement is verified by vendor documentation (no specific vendor document is referenced). We could not find the verification in the vendor documents provided. Later we were told that it was included in vendor documents not available to us. This may have been tested in the site acceptance test, but from the data, we could not verify an actual test. I assume the 2 second requirement is for all channels, but it is not stated as such.

***WSRC Response / Actions to Improve (Accepted)***

The system's reaction time to an input is basically a function of its scan time (i.e. scan time = input scan + logic solution + driving of outputs + system overhead). With the amount of modules installed in the large TEF system, the scan time for system is roughly .3 seconds. The vendor's product description manual for its processor module provides an explanation of the factors involved in the scan time interval (see pages 15-18 of attached PDF, Issue 10, June 2003 PD-8110B Trusted Processor manual). Scan time for the processor is configurable (within the restrictions of the system's I/O quantities) and based upon the two second response time specified in the TEF SDD, WSRC personnel have set the scan time at one second maximum. A processor scan time in excess of this value will produce a system error. No such errors occurred during the testing process for either system nor has one occurred in the 234-7H system since it has been in service. It was an oversight on our part when we failed to document this one second, maximum scan time setting. In future testing, we will generate a printout of the configuration screen which shows the current scan time and include this printout as part of the system's test record.

3. Concern is expressed that the system being developed (WPS) had over 100 changes to the requirements. Explain the number of changes in the TEF WPS project.

***WSRC Response / Explanation***

These process changes have resulted in modifications to the monitoring requirements for the facility in order to maintain safe working conditions. These two factors, in addition to utilizing specialized field instrumentation from multiple vendors, have been the main driving forces for the many design changes. Also, WSRC is using some of this equipment in other facilities and lessons learned from those are applied when applicable.

4. Comment: Additional time to review the volume of documents presented should be considered.



## 4.0 Detailed Results

---

### 4.1 Software Quality Assurance Program

---

**Criteria Met:** YES

#### *Software Quality Assurance Policies, Process, Procedures and Standards*

**Objective:**

Software quality activities evaluated for applicability to the Safety System Software and Firmware Software for Safety Systems, to the appropriate level of rigor, and implementation.

**Results:**

Software quality activities are evaluated for applicability to the software and are defined to the appropriate level of rigor, and are implemented. Software quality activities and software practices for requirements management, software design, configuration management, verification, testing and documentation are evaluated and established at the appropriate levels for Safety System Software and Firmware. Effective implementation was demonstrated by the reviews of the various documents listed in attachment 5.3 & 5.4, discussions with the responsible engineers and review of the configuration change control process.

A well defined process is in place for SQA (Quality Assurance Procedure / Software Quality Assurance 20-1 and E7 Engineering Manual) and it includes Safety System Software and Firmware. The program is based on regulatory guides and standards. SRS has a defined classification process for all software that is documented and executed. The site uses a graded approach and covers both purchased and developed hardware and software. Both are well defined and executed. The SQA program covers the entire lifecycle from concept through retirement for Safety System Software and Firmware. The SQA process is connected to the procurement and security processes.

SQA requirements are included with the system level QA requirements

## Software Quality Assurance Data

---

### 4.2 Software Requirement Description

---

**Criteria Met:** YES

**Objective:**

Instrumentation & Control (I&C) software functions, requirements, and their bases are defined and documented.

**Results:**

The WPS and TCON software systems were reviewed for appropriate SQA processes including functions, requirements, and their bases are defined and documented. Both

systems have proper functional and performance requirements that are complete, correct, consistent, clear, testable, and feasible. The software requirements are well documented and consistent with the system safety basis. The software requirements description (SRD) is controlled and maintained for each system (attachment 5.2). Each requirement is uniquely identified and defined such that it can be objectively verified and validated.

The team traced two safety requirements through the SQA documents and determined that there was a logical path through software design, development testing and installation for the WPS. Testing was conducted to verify appropriate software response and documented. Some inconsistencies were noted in the documented test data; however these did not affect the test results, (see Section 3.2 Noted Items for details).

The Software Quality Assurance Plan for Tritium Process Control addresses the requirements for Safety Significant Software. This plan defines the requirements through SRS Quality Assurance Program Documents and Engineering Manuals that specify detailed requirements consistent with classification of the software. These processes were followed for the two systems reviewed.

---

### **4.3 Software Design Description**

---

**Criteria Met: YES**

***Objective:***

The software design description (SDD) depicting the logical structure, information flow, logical processing steps, and data structures, are defined and documented.

***Results:***

The Design Description for Software (DDS) for the WPS depicts the appropriate logic structure, information flow, processing steps, and data structures that are consistent with its function and safety class. All software related requirements are implemented in the design. All design elements are traceable to the requirements and the design is correct, consistent, and clearly presented.

The Design Agency develops a Requirements Traceability Matrix (RTM) in accordance with site QA/SQA procedures. The requirements traceability matrix is required to ensure the flow-down of design requirements through the development and implementation of the software. Procedures were recently revised to provide guidance on preparing the RTM earlier in the lifecycle to enhance the current process. This part of the SQA graded approach based on classification. The RTM is required in the Design phase but can also be started in the Requirements phase for Safety System Software.

Vendor documentation was thorough and well prepared. SRS observes the vendor tests at the vendor before accepting the software and associated equipment. Design requirements were clearly identified in the vendor manual and logic drawings developed. The 2 second alarm time was traced through from the design requirements to the acceptance testing supplied from the vendor, although it was not contained in the original test package. (See 3.2 Noted Item # 2 above).

---

#### **4.4 Software Testing, Acceptance and Turnover (SRS terminology)**

---

**Criteria Met: YES**

(Verification and Validation to others)

***Objective:***

The Testing, Acceptance and Turnover(placed in production operation) process and related documentation for Safety System software and Firmware are defined and maintained to ensure that (a) the software adequately and correctly performs all its intended functions; and that (b) the software does not perform any adverse unintended function.

***Results:***

The Testing, Acceptance and Turnover process and related documentation for Safety System Software and Firmware is defined and maintained and ensures that (a) the software adequately and correctly performs all its intended functions; and that (b) the software does not perform any adverse unintended function. The software requirements and software designs were verified and validated for correct operation using testing, observation, or inspection techniques. Relevant abnormal conditions were evaluated for mitigating unintended functions through testing, observation, or inspection techniques.

The Design Agency is required to develop software testing per the requirements of the SQA procedures, ensuring that test cases are traceable to requirements and design. The software testing is required to demonstrate that the software:

- Adequately and correctly performs all intended functions,
- Properly handles abnormal conditions and events as well as credible failures,
- Does not perform adverse unintended functions, and
- Does not degrade the system either by itself, or in combination with other functions or configuration items to ensure that the software satisfies requirements,
- Integrity is not compromised on the target system and
- Is accepted for operational use

These processes also require verification and validation of the software test cases. SRS utilizes independent review as the term applied to ensure that verification is performed by a separate person. This process requires that the results of the independent review must be documented and the individual identified. The Design Authority ultimately verifies that all required independent reviews of software test cases were performed and approves all software test documentation.

---

## 4.5 Software User Documentation

---

**Criteria Met: YES**

***Objective:***

Software documentation is available to guide the user in installing, operating, managing, and maintaining the Safety System software and Firmware.

***Results***

Documentation and training is available. Access to software and documentation is limited to users that are approved and trained. Training is provided or planned and coordinated. Simulators are and will be used to ensure training for the applications of the Safety System software and Firmware. Documentation is controlled within the configuration management process to ensure the correct version is used.

---

## 4.6 Software Configuration Management

---

**Criteria Met: YES**

***Objective:***

Software components and products are identified and managed, and changes to those items are controlled.

***Results:***

Software components and products to be managed are identified by procedures and a system is established to manage the modification and installation of new versions. Procedures for modifications to those software products are followed.

Configuration management (change control) is utilized on Design Authority approved changes to computer programs for all the configuration items in the software configuration index in accordance with the requirements established in the SQAP. The Software Configuration Management Database lists all the systems covered under the SQAP. The configuration items are listed for each system along with design and related documentation.

Software modifications are strictly controlled in accordance with the Modification Control Procedure. Forms are used if the change requires source code modification. Software Modification Package Forms are used for all safety system software changes.

Two software modification packages were reviewed for consistency with requirements. These modification packages addressed software changes to the WPS. The forms and the packages provide a structured approach to accomplishing the change and included requirements, justifications, and independent reviews. A checklist is provided for the engineer to determine whether or not the change involves a number of different aspects of operation, engineering, acquisition or training. Software testing results were attached to the modification package and verified.

---

## 4.7 Software Quality Assurance

---

**Criteria Met:** YES

***Objective:***

Software quality activities are evaluated for applicability to the Safety System software and Firmware, defined to the appropriate level of rigor, and implemented.

***Results:***

Software Quality Assurance is applicable to Safety System Software at the appropriate level of rigor, and is implemented. Software quality activities and software practices for requirements management, software design, configuration management, verification, testing and documentation are evaluated and established at the appropriate levels for these systems. Effective implementation was demonstrated by the performance based reviews of the flow-down of design requirements through the various documents and the configuration change control process.

The Tritium Process Control Software Quality Assurance Plan, Revision 1 identifies a set of requirements that assured appropriate SQA for the software reviewed. It is the facility implementing procedure for Manual E7, "Conduct of Engineering and Technical Support," Procedure 5.03, "Software Quality Assurance Plan." A strength of this plan is that it is written to apply software quality assurance to all levels of software and is not strictly limited to nuclear safety software. It also defines roles and responsibilities for those involved in SQA processes.

---

## 4.8 Software Procurement

---

**Criteria Met:** YES

***Objective:***

Acquired software meets the applicable level of quality to ensure the safe operation of the system.

***Results:***

SRS procedures cover purchased, acquired and developed Safety System Software and Firmware. The SRS procedures were implemented for these systems and the documentation reviewed supports the SQA requirements. The SRS SQA program is connected to the SRS Procurement process and based on the software classification; the required procurement actions are implemented. This connection ensures that procured Safety System Software is purchased from qualified vendors. The Factory and Site Acceptance test processes also ensure quality.

---

## **4.9 Software Problem Reporting and Corrective Action**

---

**Criteria Met: YES**

***Objective:***

A process for Safety System software and Firmware problem reporting is established, maintained, and controlled, including notification of errors, failures, and corrective action development.

***Results:***

The SRS QA/SQA program and procedures cover problem reporting and corrective actions. Vendor related problems with purchased products are reported, reviewed and applied as required. Procedures to report problems, notify appropriate individuals, and implement corrective actions are included with system level problem reporting and other procedures.

---

## **5.0 Attachments**

---

- 5.1 Background information on Assessment Team**
- 5.2 Lines of Inquiry Summary**
- 5.3 Assessments Documents Reviewed List**
- 5.4 WSRC SQA Procedures List**
- 5.5 Engineering Manual E7 Glossary of Terms**

---

## 5.1 Background information on Assessment Team

---

**Dennis Adams:** A retired Department Manager from Idaho National Engineering and Environmental Engineering Laboratory. Developed Man Rated Flight Hardware for NASA. As program manager I had responsibility for the Commercial Nuclear Power Emergency Response System. Designed and developed the software that controlled the three 55 ton refueling mechanisms in the Fast Flux Test Facility. I was Program Manager for \$100 M military command and control system that produced "go to war" hardware within budget and on schedule. Deputy Assessor for the two recent NNSA software assessments for the Accelerated Scientific Computing Initiative

**Elaine Doolittle:** WSRC - 11 years, Configuration Management and Engineering Automation, Procedures, Policies, and Assessments. Vice-Chair of the Site Conduct of Engineering Committee, Maintain the Conduct of Engineering Manual and Six Sigma Yellow Belt. Battelle - 4 years, System Functional Testing, Asset Lifecycle Management.  
**Education:** BS in Computer Science from Clemson University

**Vince Grosso:** Current responsibility is for the WSRC Quality Assurance Program. Work with internal and external organizations to assure Quality Assurance Rule, DOE requirements, WSRC policy, and national codes and standards are managed, interpreted, documented, understood, and implemented. Responsible Quality Assurance Functional Area Subject Matter Expert supporting the Quality Assurance Functional Program Manager. Responsibilities also include managing the WSRC Quality Assurance Policy, Quality Assurance Management Plan, Corporate Quality Assurance Procedures, and secretary for the WSRC Quality Managers Committee. Participated in DOE HQ Quality Assurance evaluations at other DOE complex sites, and have also performed WSRC audits, assessments, and surveillances. Commercial nuclear experience includes construction, start-up, operations, outages, and D&D / recovery operations at TMI. Past 20+ years: Government Nuclear – WSRC / Commercial Nuclear

**Education:** Master of Science Human Resource Management / Masters of Business Administration / Bachelors and Associates in Science and Math

**Active Memberships:** National Management Association

**Chip Lagdon:** Chip Lagdon is the Director for the Office of Quality Assurance Programs in the Office of Environment Safety and Health. In this capacity, he is responsible for Quality Assurance Programs within the Department. Presently, Mr. Lagdon is the lead for Defense Nuclear Facilities Safety Board Recommendation 2002-1 on Software Quality Assurance and is managing the completion of over 29 commitments by line organizations and the field. He also has program responsibility for the Radiation & Environmental Services Laboratory in Idaho, the Voluntary Protection Program, the Quality Assurance Order, the Analytical Services Program and the DOE Laboratory Accreditation Program.

**Keith Morrell:** Westinghouse Savannah River Company Technical Advisor. I have responsibility for the Software Quality Assurance program at the company level. Work with internal and external organizations to assure Software Quality Assurance requirements, policy and standards are implemented, maintained and improved from conception through retirement. I have worked in Government Nuclear, Commercial Nuclear, and Oil & Gas Industry with 25+ years in the technology business area.  
**Education:** BS in Business Administration from Greensboro College  
**Active Memberships:** American Society of Mechanical Engineers – NQA, Nuclear Information Technology Strategic Leadership, Software Computing Consortium (CMU)

**Gregg Nelson:** Began career with the National Nuclear Security Administration in September 2001. Currently, he is the Savannah River Site Office Point of Contact for Information Technology, Cyber Security and Software Quality Assurance.  
**Education:** BS in Electrical Engineering from the University of South Carolina.  
**Active Memberships:** National Society of Black Engineers



## 5.2 Lines of Inquiry Summary

<b>SRS/ WSRC - QAIP / IP 4.2.3 Assessment of Safety System Software and Firmware for I&amp;C</b> <b>System: TEF Worker Protection System (WPS) &amp; TCON    Classification: SS</b>					
Q#	Review Questions	Yes/No	Validate by Standards/Requirements and Process/Procedures	Verify by Objective Evidence	Institutionalized Yes/No
	This column lists the review questions tailored for SRS business. CRAD document 4.2.3.1 will be used as a guide for the review and report generation.	Yes, where review questions can be answered positively and objective evidence exists; No, otherwise.	Identify the applicable standards, requirements, and associated process/ procedures applied that result in effective implementation and production of the objective evidence.	This column identifies the objective evidence where it exists (e.g., records, reports, work packages, e-mails, meeting minutes, and other documents). And TEF Worker Protection Specific Documents as required	This column indicates if the site processes / procedures were applied.

0	<p>Questions #0 look at the procedures and process in place at SRS and reference the standards they are based on.</p> <p>Are the site level QA/SQA procedures applicable for Safety System Software?</p>	YES	<p>10CFR830 Subpart A Quality Assurance, DOE Order 414.1A Quality Assurance, ASME NQA-1-1997, ASME NQA-1a-1999, ASME NQA-1-2000 QUALITY ASSURANCE REQUIREMENTS FOR NUCLEAR FACILITY APPLICATIONS, DOE/AL QC-1, Rev. 9 DOE/AL Quality Criteria (QC-1), DOE/RW-0333P, Rev 6 Quality Assurance Requirements and Description for the Civilian Radioactive Waste Management Program, ANSI/ASQC E4 SPECIFICATIONS AND GUIDELINES FOR QUALITY SYSTEMS FOR ENVIRONMENTAL DATA COLLECTION AND ENVIRONMENT TECHNOLOGY PROGRAMS, Additional IEEE Standards are applied via ASME NQA and referenced in procedures</p>	<p>WSRC 1Q Quality Assurance Manual procedure: 20-1 Software Quality Assurance / WSRC E7 - Conduct of Engineering Manual procedures: 2.25 Functional Classifications, 2.31 Engineering Calculations, 2.40 Design Verification and Checking, 5.01 Software Engineering and Control, 5.03 Software Quality Assurance Plan, 5.04 Software Project Management Plan, 5.05 Software Classification, 5.07 Evaluation of Existing and Acquired Software, 5.10 Software Requirements, 5.20 Software Design and Implementation, 5.40 Software Testing, Acceptance, and Turnover, 5.61 Engineering &amp; Scientific Software Distribution and Control, 5.62 Computer Program Modification Tracker, 5.80 Data Management. Additional WSRC QA, SQA, Security, Records Management and Procurement procedures apply and are used as required. WSRC Quality Assurance management Plan (QAMP). In reviewing selected documents it is apparent that there is a well defined software process in place that is well based in regulatory guides and standards. There is participation by SRS in national regulatory bodies and personnel are well aware of the latest updates in regulatory guides and standards.</p>	<p>YES. The software processes and procedures are applicable to safety system software. They follow accepted national regulatory guides and standards. SRS is also represented on several software/safety committees of national stature.</p>
---	--	-----	---	---	---

0a	Do the same procedures documented in QAIP 3.3 action apply ?	YES	See attached QAIP 3.3 report	as required	Yes, the procedures documented in QAIP 3.3 apply and there is evidence that quality assurance methods are effectively implemented for the design, procurement, construction, fabrication and operation of safety systems. Quality assurance actions are developed and deployed but there is little evidence of quality measurement or quality metrics being used to quantitatively measure results.
0b	Does the site have a defined classification process for safety software ?	YES	WSRC 1Q Quality Assurance Manual procedure: 20-1 Software Quality Assurance / WSRC E7 - Conduct of Engineering Manual procedures: 2.25 Functional Classifications, 5.05 Software Classification	follow the site QA / SQA program / processes	Yes, the site does have a defined classification process for safety software that is inherent in following their procedures.
0c	Does the site have a graded approach to software, that includes safety software ?	YES	WSRC 1Q Quality Assurance Manual procedure: 20-1 Software Quality Assurance / WSRC E7 - Conduct of Engineering Manual procedures: 2.25 Functional Classifications, 5.01 Software Engineering and Control, 5.03 Software Classification	follow the site QA / SQA program / processes	Yes, the site uses a graded approach to a defined software processes. There was a clear distinction in process followed. The processes were well defined and being followed by the engineers and development personnel.

0d	Do the QA/SQA procedures cover the entire lifecycle of the safety system software from concept through retirement ?	YES	WSRC 1Q Quality Assurance Manual procedure: 20-1 Software Quality Assurance / WSRC E7 - Conduct of Engineering Manual procedures: 2.25 Functional Classifications, 2.31 Engineering Calculations, 5.01 Software Engineering and Control, 5.03 Software Quality Assurance Plan, 5.04 Software Project Management Plan, 5.05 Software Classification, 5.07 Evaluation of Existing and Acquired Software, 5.10 Software Requirements, 5.20 Software Design and Implementation, 5.40 Software Testing, Acceptance, and Turnover, 5.61 Engineering & Scientific Software Distribution and Control, 5.62 Computer Program Modification Tracker, 5.80 Data Management.	follow the site QA / SQA program / processes	Yes, the system lifecycle is covered through retirement. During our review we found evidence of software requirements definition, requirements traceability, an SDD, testing, verification, factory and site acceptance tests, configuration management and other lifecycle elements.
----	---	-----	---	--	---

0e	Do the QA/SQA procedures cover the Procurement process for Safety System Software?	YES	WSRC 1Q Quality Assurance Manual procedures: 20-1 Software Quality Assurance, Procedure 2-3, "Control of Research and Development Activities", Procedure 2-7, "QA Program Requirements for Analytical measurement Systems", Procedure 7-3, "Commercial Grade Item Dedication", Procedure 12-1, "Control of Measuring and Test Equipment", Procedure 15-1, Control of Nonconforming Items" / WSRC Procurement Procedures: Manual 7B, Procurement Management Manual, Manual 3E, Procurement Specification Procedure Manual.	follow the site QA / SQA program / processes	Yes, these two systems use a certified triply redundant processor that is programmed through screen manipulation of icons for logic elements. We found evidence of factory acceptance and site acceptance tests and procedures for Commercial Grade Item Dedication being followed as well as control of the procured equipment.
----	--	-----	---	--	--

## 1 REQUIREMENTS

WSRC 1Q Quality Assurance  
Manual procedure: 20-1  
Software Quality Assurance /  
WSRC E7 - Conduct of  
Engineering Manual procedures:  
5.03 Software Quality Assurance  
Plan, 5.10 Software  
Requirements,

specific system documents were reviewed

Yes, we found evidence of enumerated requirements that are traceable through the software lifecycle from concept to implementation and test. Furthermore a requirement traceability matrix is being used. I have some concern that the system being developed (WPS) had over 100 changes to the requirements. It would appear that the requirements were not very well thought out. Hopefully these changes were caught early enough to avoid extensive rework.

1a	Is WPS software covered by a Software Quality Assurance Plan (SQAP), and is the SQAP a lifecycle document ?	YES	See Requirements	WPS software is controlled via SQAP B-SQP-H-00030 Rev. 1. It is a lifecycle document based on WSRC E7 Procedure 5.03, Software Quality Assurance Plan.	YES, The WPS software is covered by a Software Assurance Plan and the SQAP is a lifecycle document. Note that we were able with the help of an engineer to track a change from the requirement change to the implementation of the change, and finally the test of that change. Contents and format were following current version of SQA procedure. Defined deliverables verified.
----	---	-----	------------------	--	--

1b	Is there a Requirements Document that identifies expected WPS Functionality	YES	See Requirements	B-RS-H-00074 for TEF WPS, B-RS-H-00116 for TCON WPS.	YES, During the review we looked at the requirements document. Note that the requirements for this logic system are expressed as a logic diagram which better meets the needs of design engineers than a text document. The logic diagram also lends itself better to the icon manipulation method used for this equipment. Documents were approved. Documents identify Critical and Non-Critical requirements. Acceptance criteria defined for TCON. TEF acceptance criteria needs defined. (note TEF in development)
1c	Is the WPS Requirements Document appropriately reviewed, approved, issued, and under change control?	YES	See Requirements	All changes, reviews, and approvals are controlled via the SQAP document.	It was apparent that all documents were reviewed and signed off on, and under change control. We looked at Rev 0, that was marked as for information only and Rev 2 that was marked as a working copy of the requirements



3/18/2004

FSS-TQS-2004-00001

1d	Are the WPS requirements consistent with the Safety Basis ?	YES	See Requirements	The system's Design Authority is required to check for agreement between the system's requirements and the facility's Safety Basis. See reference J-SYD-H-00003.	Yes. We saw requirements documents signed off by the design authority respect to the facility safety basis.
----	---	-----	------------------	--	---

1e	Are WPS requirements clearly identified, traceable and testable?	YES	See Requirements	B-RS-H-00074 requirements document for TEF WPS and B-RS-H-00116 for TCON WPS.	<p>YES, We saw that a traceability matrix was being used. I did have some problems with the site acceptance test in that some test data sheets were not signed, dated, and some of the columns were not filled out. If these particular columns are not applicable, they should be marked as "NA". Also many of the page numbers on the test data sheets were not legible. Also there was a requirement that input to output of the controller be within 2 seconds. The documentation says that this requirement is verified by vendor documentation (no specific vendor document is referenced). We could not find the verification in the vendor documents provided. Later we were told that it was included in vendor documents not available to us. This may have been tested in the site acceptance test, but from the data, we could not verify an actual test. I assume the 2 second requirement is for all channels, but it is not stated as such.</p>
----	--	-----	------------------	---	--

1f	Is the WPS Requirements Document a Lifecycle document to be maintained until system retirement ?	YES	See Requirements	Software is controlled via SQAP B-SQP-H-00030 Rev. 1. It is a lifecycle document based on WSRC E7 Procedure 5.03, Software Quality Assurance Plan.	Yes. The site's document control function has identified RS document codes as being maintained until system retirement.
2	DESIGN and DEVELOPMENT		WSRC 1Q Quality Assurance Manual procedure: 20-1 Software Quality Assurance / WSRC E7 - Conduct of Engineering Manual procedures: 5.03 Software Quality Assurance Plan, 5.04 Software Project Management Plan, 5.05 Software Classification, , 5.10 Software Requirements, 5.20 Software Design and Implementation, 5.40 Software Testing, Acceptance, and Turnover,	Specific system documents	YES
2a	Is WPS software design documented in a Design Description - Software (DDS) ?	YES	See Design and Development	B-DD-H-00036 TEF B-RS-H-0116 TCON	YES, There is a Design Document, note that the software design uses logic design to better specify the logic tree need for implementation. Documents follow site procedures.
2b	Is the DDS reviewed, approved and consistent with governing procedures?	YES	See Design and Development	SQAP, B-SQP-H-00030	Yes, the software design document review and approval is controlled via the system's SQAP, B-SQP-H-00030. Sign off and verification reviews were evident.

2c	Are all approved WPS requirements addressed in the WPS design ?	YES	See Design and Development	See document B-DD-H-00036 for TEF WPS and B-DD-H-00035 for TCON WPS	Yes. The DDS references the requirement(s) implemented by each design entity. See document B-DD-H-00036 for TEF WPS and B-DD-H-00035 for TCON WPS. During the time allocated for the review, it was impossible to check all requirements one by one. We did go through a requirement change from the change documentation to implementation and check. I noted that all documents were reviewed and signed off. Also there was a requirements traceability matrix being used to trace requirements through the lifecycle.
2d	Is WPS design traceable to requirements ?	YES	See Design and Development	See RTM B-RTM-H-00019. for TEF WPS and B-RTM-H- 00010 for TCON WPS	Yes. Requirements were numbered and a traceability matrix is being utilized.

3	SOFTWARE TESTING, ACCEPTANCE AND TURNOVER Note: TEF WPS is still in the Design and Implementation Phase. All references from this point forward apply only to the TCON WPS.		WSRC 1Q Quality Assurance Manual procedure: 20-1 Software Quality Assurance / WSRC E7 - Conduct of Engineering Manual procedures: 5.03 Software Quality Assurance Plan, 5.40 Software Testing, Acceptance, and Turnover,	Specific system documents	YES
3a	Will the testing be done under a Test Plan that has been independently reviewed, approved and issued?	YES	See Software Testing, Acceptance and Turnover	SQAP B-SQP-H-00030 specifies review and approval process. TCON test plan B-STP-H-00123 reviewed	Yes. SQAP B-SQP-H-00030 specifies review and approval process. Note: TEF WPS is still in the Design and Implementation Phase. All references from this point forward apply only to the TCON WPS. Test plan in place for the system. There are site and factory acceptance test performed on the hardware and software (system software for the site test).
3b	Will the testing prove that the requirements have been met and implemented correctly ?	YES	See Software Testing, Acceptance and Turnover	Software Test Plan points to the requirement proven by the Software test case(s).	Yes. Information within the Software Test Plan points to the requirement proven by the Software test case(s). Acceptance Criteria is stated for each software test case.

3c	Does the Test Plan include testing for system response to abnormal conditions that may occur during operations?	YES	See Software Testing, Acceptance and Turnover	Additional test cases are developed to address abnormal conditions.	YES
3d	Does the Test Plan require an independent review and approval of the test results?	YES	See Software Testing, Acceptance and Turnover	SQAP B-SQP-H-00030	Yes. SQAP specifies review and approval process for test plans.
4	OPERATIONS AND MAINTENANCE		WSRC 1Q Quality Assurance Manual procedure: 20-1 Software Quality Assurance / WSRC E7 - Conduct of Engineering Manual procedures: 5.01 Software Engineering and Control, 5.03 Software Quality Assurance Plan, 5.40 Software Testing, Acceptance, and Turnover, 5.61 Engineering & Scientific Software Distribution and Control, 5.62 Computer Program Modification Tracker, 5.80 Data Management.	Specific system documents	YES
4a	If user documentation is required, will it be available at system acceptance?	YES	See Operations and Maintenance	Yes, user documentation is required for all SS class systems - Provided via system console and logic diagrams. B-UG-H-00032 for TEF	Yes, user documentation is required for all SS class systems - Provided via system console and logic diagrams.
4b	Will WPS configuration items be identified to enable configuration management?	YES	See Operations and Maintenance	Yes, all system configuration items are identified in the Software Configuration Management Database (SCMDB).	Yes, all system configuration items are identified in the Software Configuration Management Database (SCMDB).

4c	Will WPS software be placed under configuration management before being turned over to Operations?	YES	See Operations and Maintenance	Yes. Documentation of the system under configuration management is found in the SCMDB. Software is in configuration management and a change comparison process is used to verify that the changed correct software is being used.	Yes. Documentation of the system under configuration management is found in the SCMDB. Software is in configuration management and a change comparison process is used to verify that the changed correct software is being used.
4d	Will WPS software be modified according to E7 and / or approved SQAP?	YES	See Operations and Maintenance	Software Modification Packages B-SMPk-H-00505 and B-SMPK-H-00533.	YES, We walked through the change process with an engineer to verify the methods and traceability of the change.
4e	Will there be a process to handle software problem reporting and corrective action ?	YES	See Operations and Maintenance	See section 5.0 of SQAP B-SQP-H-0030. .	YES, There is a process to handle problem reporting and corrective actions. There is also a notification process that alerts others of the impact of the change or other items that are affected by the change
5	QA/SQA Document process ?	YES	WSRC 1Q Quality Assurance Manual procedure: 17-1 "Quality Assurance Records Management"	QAP 20-1 and E7 procedures reference / follow the site records/ document management procedures.	There is a defined and deployed QA/SQA process in place. Note that engineers are trained and aware of the processes and are using the prescribed processes for QA/SQA.
6	List any recent (past two years) related assessments & results		Tiger Team Readiness Assessment of 234-7H facility	Tiger Team 7H Action Item Listing	DP Specific, One minor software related action item closed.

3/18/2004

FSS-TQS-2004-00001

DNFSB Review of TEF WPS  
project including SQA 1/15/03  
P&CT self Assessment program  
for has reviewed SQA

Positive results, RTM modification

2001, 2002 ,2003.

YES

YES, Looked at some  
of the self -assessment  
documents were QA  
documents and  
processes were  
compared to  
commercial nuclear  
facilities. A really good  
practice. Results were  
documented as  
favorable.

Also note that the DNFSB is interested in training.  
SRS uses the automated "train" system to track  
training requirements for personnel.



### 5.3 Assessments Documents Reviewed List

Rev	Date	Number	Name
1	5/1/2001	B-SQP-H-00030	Tritium Process Control SQAP
0	2/27/2002	B-TPR-H-00105	234-7H Worker Protection System TMR Factory Acceptance Test
0	1/22/2002	U020122241004	TUV Product Certificate for Safety Related Programmable Electronic System
3.2	4/4/2002	012-10032636	Report to the Certificate for the TUV Product Certificate for Safety Related Programmable Electronic System
0	9/30/2003	E-CGD-H-00699	Replacement Item Evaluation/Commercial Grade Item Dedication Form - 24 V.D.C. AT 20 Amps Power Supply
0	9/30/2003	E-CGD-H-00700	Replacement Item Evaluation/Commercial Grade Item Dedication Form - Trusted Communications Module for the Safety Qualified, Programmable Logic Controller (PLC)
0	9/30/2003	E-CGD-H-00701	Replacement Item Evaluation/Commercial Grade Item Dedication Form - ICS Triplex Safety PLC for the 234-7H Health Protection System
1	2/17/2004	B-RS-H-00120	Tritium Process Control RSS/DDS for 234-7H WPS Process Simulation
1	2/17/2004	B-STP-H-00137	Tritium Process Control STP for 234-7H WPS Process Simulation
0	9/8/2003	B-ESR-H-00006	TUV Requirements for Maintenance Overrides
0	2/16/2004	B-UG-H-00033	System Management Guide for PLC Systems
0	2/17/2004	B-SMPK-H-00505	Software Modification Package
0	2/16/2004	B-SMPK-H-00505	Software Modification Package Alarm Bypass
0	2/17/2004	B-SMPK-H-00533	Software Modification Package Lights/Horn Modification
0	2/16/2004	B-SMPK-H-00533	Software Modification Package Lights/Horn Modification
0	2/17/2004	B-SMPK-H-00505	Software Modification Package Alarm Bypass
	2/17/2004	QAIP 3.3	Verification and Validation of Quality Assurance Programs
	2/16/2004	J-DCF-H-03778	TAM 100 High Activity Alalog Alarm
	1/17/2003	E-DCF-H-05962	7H, PWR Feed from Panel
	8/28/2003	J-DCF-H-03778	TAM 100 High Activity Alalog Alarm
	2/17/2004	J-DCF-H-03778	TAM 100 High Activity Alalog Alarm
	2/17/2004	J-DCF-H-03778	TAM 100 High Activity Alalog Alarm
	8/6/2003	J-DCF-H-03765	234-7H TAM Bypass Light
	2/17/2004	J-DCF-H-03765	234-7H TAM Bypass Light
	2/17/2004	J-DCF-H-03765	234-7H TAM Bypass Light
0	11/10/2003	TP-MTF-00719	234-7H Air Monitor System Test
2	2/11/2004	B-STP-H-00123	Tritium Process Control Worker Protection System Software Test
2	11/17/2003	B-STP-H-00123	Tritium Process Control Worker Protection System Software Test
1	9/8/2003	B-STP-H-00123	Tritium Process Control Worker Protection System Software Test
1	7/16/2003	B-STP-H-00123	Worker Protection System Software Plan
1	9/8/2003	B-STP-H-00123	Tritium Process Control Worker Protection System Software Test
0	6/5/2003	B-STP-H-00123	Tritium Process Control Worker Protection System Software Test
0	6/5/2003	B-STP-H-00123	Tritium Process Control Worker Protection System Software Test
0	12/8/2003	B-STP-H-00176	Tritium Process Control Worker Protection System Software Test

2	2/17/2004	B-DD-H-00035	Tritium Process Control Worker Protec. Design Document for Software
2	2/11/2004	B-DD-H-00035	Tritium Process Control Worker Protec. Design Document for Software
1	9/8/2003	B-DD-H-00035	Tritium Process Control Worker Protec. Design Document for Software
1	2/11/2004	B-DD-H-00035	Tritium Process Control Worker Protec. Design Document for Software
0	6/5/2003	B-DD-H-00035	Tritium Process Control Worker Protec. Design Document for Software
0	6/5/2003	B-DD-H-00035	Tritium Process Control Worker Protec. Design Document for Software
2	2/17/2004	B-RTM-H-00010	Tritium Process Control Requirements Traceability Matrix
2	2/11/2004	B-RTM-H-00010	Tritium Process Control Requirements Traceability Matrix
1	9/8/2003	B-RTM-H-00010	Tritium Process Control Requirements Traceability Matrix
1	9/8/2003	B-RTM-H-00010	Tritium Process Control Requirements Traceability Matrix
0	6/5/2003	B-RTM-H-00010	Tritium Process Control Requirements Traceability Matrix
0	6/5/2003	B-RTM-H-00010	Tritium Process Control Requirements Traceability Matrix
2	2/11/2004	B-RS-H-00116	Tritium Process Control WPS Requirements Specification for Software
2	2/17/2004	B-RS-H-00116	Tritium Process Control WPS Requirements Specification for Software
1	9/8/2003	B-RS-00116	Tritium Process Control WPS Requirements Specification for Software
1	9/8/2003	B-RS-00116	Tritium Process Control WPS Requirements Specification for Software
0	6/5/2003	B-RS-00116	Tritium Process Control WPS Requirements Specification for Software
0	6/5/2003	B-RS-00116	Tritium Process Control WPS Requirements Specification for Software
2		B-RS-00116	Tritium Process Control WPS Requirements Specification for Software
0	9/30/2003	B-TPR-H-00108	Worker Protection System TMR
0	9/30/2003	E-CGD-H-00699	ICS Triplex Safety PLC for the Health Protection System
3	2/17/2004		Tritium Facility Modernization 8 Consolidation Project
	2/11/2004		Building 234-H Modifications by Project S-7726
6	5/11/2001	J-SYD-H-00003	System Description Document ICS Project S-6901
2	10/21/2003	J-TRT-H-00026	CLWR - TEF Continuous Air Monitoring System Interlock and Effects Database Report Logic
1	5/12/2001	J-TRT-H-00023	Room Oxygen Monitoring
1	5/9/2001	J-TRT-H-00011	Module Environmental Monitoring System Interlock
1	5/12/2001	J-TRT-H-00025	Project S-6091 CLWR-Tritium Extraction Facility Air Monitoring System Interlock and Effects Database Report - Logic Descriptions
0	6/25/2002	B-TPR-H-00111	Tritium Extraction Facility Worker Protection System Factory Acceptance Test
0	1/6/2003	E-CGD-H-00715	Replacement Item Evaluation/Commercial Grade Item Dedication Form - Module, Main Processor
0	1/6/2003	E-CGD-H-00716	Replacement Item Evaluation/Commercial Grade Item Dedication Form - Module, Expander Interface
0	1/6/2003	E-CGD-H-00717	Replacement Item Evaluation/Commercial Grade Item Dedication Form - Module, Communications
0	1/6/2003	E-CGD-H-00719	Replacement Item Evaluation/Commercial Grade Item Dedication Form - Module, Analog Input
0	1/6/2003	E-CGD-H-00720	Replacement Item Evaluation/Commercial Grade Item Dedication Form - Module, Output

0	1/6/2003	E-CGD-H-00721	Replacement Item Evaluation/Commercial Grade Item Dedication Form - Module, Input
0	1/6/2003	E-CGD-H-00723	Replacement Item Evaluation/Commercial Grade Item Dedication Form - Power Supply, 24 V.D.C.
0	12/10/2002	B-TPR-H-00124	Tritium TMR Test Procedure
1	10/1/2003	B-TPR-H-00124	Tritium TMR Test Procedure
0	1/22/2002	U020122241004	TUV Product Certificate for Safety Related Programmable Electronic System
3.2	4/4/2002	012-10032636	Report to the Certificate for the TUV Product Certificate for Safety Related Programmable Electronic System
1 Draft	5/12/2003	B-RS-H-00074	Tritium Process Control TEF Worker Protection System Requirements Specification for Software
0	12/9/2002	email	Comments and Comment Resolutions for WPS IR-2 Review of B-RS-H-00074 Rev. 0
0	8/1/2002	B-RS-H-00074	Tritium Process Control TEF Worker Protection System Requirements Specification for Software
0 Draft	Draft	B-RTM-H-00019	Tritium Process Control TEF Worker Protection System Requirements Traceability Matrix
0 Draft	5/12/2003	B-DD-H-00036	Tritium Process Control TEF Worker Protection System Design Document for Software
0	12/11/2002	E-DCF-H-05907	Design Change Form Miscellaneous Storage Module Deletion
1		JJQH1484	CLWR-Tritium Extraction Facility Tritium Processing Building Worker Protection System H-264000-WPS-CAB-98 Termination Cabinet Arrangement Sheet 1 of 4
1		JJQH1485	CLWR-Tritium Extraction Facility Tritium Processing Building Worker Protection System H-264000-WPS-CAB-98 Termination Cabinet Arrangement Sheet 3 of 4
1		JJQH1486	CLWR-Tritium Extraction Facility Tritium Processing Building Worker Protection System H-264000-WPS-CAB-1060 Termination Cabinet Arrangement
3		JJQH1487	CLWR-Tritium Extraction Facility Remote Handling Building Worker Protection System H-264002-WPS-CAB-1050 Termination Cabinet Arrangement Sheet 1 of 3
2		JJQH1488	CLWR-Tritium Extraction Facility Remote Handling Building Worker Protection System H-264002-WPS-CAB-1050 Termination Cabinet Arrangement Sheet 2 of 3
1		JJQH1489	CLWR-Tritium Extraction Facility Tritium Processing Building Worker Protection System H-264000-WPS-CAB-1059 Termination Cabinet Arrangement
1		JJQH1490	CLWR-Tritium Extraction Facility Tritium Processing Building Worker Protection System H-264000-WPS-CAB-1056 Termination Cabinet Arrangement Sheet 1 of 2
1		JJQH1491	CLWR-Tritium Extraction Facility Tritium Processing Building Worker Protection System H-264000-WPS-CAB-1057 Termination Cabinet Arrangement Sheet 1 of 2
1		JJQH1492	CLWR-Tritium Extraction Facility Tritium Processing Building Worker Protection System H-264000-WPS-CAB-1058 Termination Cabinet Arrangement
1		JJQH1493	CLWR-Tritium Extraction Facility Tritium Processing Building Worker Protection System H-264000-WPS-CAB-98 Termination Cabinet Arrangement Sheet 1 of 4
1		JJQH1495	CLWR-Tritium Extraction Facility Tritium Processing Building Worker Protection System H-264000-WPS-CAB-98 Termination Cabinet Arrangement Sheet 2 of 4

4	JJQH1494	CLWR-Tritium Extraction Facility Remote Handling Building Worker Protection System H-264002-WPS-CAB- 1050 Termination Cabinet Arrangement Sheet 3 of 3
1	JJQH1496	CLWR-Tritium Extraction Facility Tritium Processing Building Worker Protection System H-264000-WPS-CAB- 1056 Termination Cabinet Arrangement Sheet 2 of 2
1	JJQH1497	CLWR-Tritium Extraction Facility Tritium Processing Building Worker Protection System H-264000-WPS-CAB- 1057 Termination Cabinet Arrangement Sheet 2 of 2

## 5.4 WSRC SQA Procedures List

Rev	Date	Number	Name
12	8/31/2003	WSRC-RP-92-225	Quality Assurance Management Plan
35	1/30/2004	WSRC-E7	Conduct of Engineering Glossary
35	1/30/2004	WSRC-E7	Conduct of Engineering Table of Contents
N/A	2/11/2004	WSRC S/RID	S/RID Compliance Data for "1Q QAP 20-1"
8	10/16/2003	WSRC 1Q 20-1	Software Quality Assurance
6	10/13/2003	WSRC E7 2.31	Engineering Calculations
3	9/28/2001	WSRC E7 2.41	Design Verification and Checking
1	7/15/2003	WSRC E7 5.01	Software Engineering and Control
2	9/19/2003	WSRC E7 5.03	Software Quality Assurance Plan
2	7/15/2003	WSRC E7 5.04	Software Project Management Plan
1	7/15/2003	WSRC E7 5.05	Software Classification
1	7/15/2003	WSRC E7 5.07	Evaluation of Existing and Acquired Software
2	7/15/2003	WSRC E7 5.10	Software Requirements
1	7/15/2003	WSRC E7 5.20	Software Design and Implementation
2	7/15/2003	WSRC E7 5.40	Software Testing, Acceptance and Turnover
1	7/15/2003	WSRC E7 5.61	Engineering & Scientific Software Distribution & Control
1	7/15/2003	WSRC E7 5.62	Computer Modification Tracker
1	8/29/2003	WSRC E7 5.80	Data Management
8	4/30/2003	WSRC E7 3.14	Design Authority Technical Reviews

## E7 - Conduct of Engineering

[Engineering Home Page](#) - [E7 Home Page](#)

### **5.5 Glossary (U) Revision No. 35 January 30, 2004**

The number in brackets refers to the procedure in which the term and its definition are introduced.

**1-level CLI** – a component or equipment number that identifies a system, component hierarchy in a five (5)-field format. [1.30]

**2-level CLI** – a component or equipment number that identifies a system, equipment, component hierarchy in a seven (7)-field format. [1.30]

**Abandoned in Place** – equipment which has been designated on technical baseline documents to be permanently abandoned with no intent to return to service. The equipment remains in the facility, is isolated from operating systems, and is not normally maintained or routinely monitored. (See WSRC Manual 2S.) [1.05]

**Acceptable Supplier/Item Performance (Verification Method 4)** - a record of acceptable performance of a supplier's commercial grade items which provides justification for WSRC to accept the item for safety use. [3.46]

**Acceptance** - For the purposes of procedure 3.46, the employment of methods to produce objective evidence which provides reasonable assurance that a Commercial Grade Item (CGI) will perform its intended safety function. Acceptance encompasses two activities: 1) receiving inspection, and 2) verification of Critical Characteristics for Acceptance (CCFAs). [3.46]

**Acceptance Criteria** – specified limits placed on characteristics of an item, process, function, or service as defined in codes, standards, or other requirement documents. [5.10]

**Accident Analysis** – see WSRC Manual 11Q, Facility Safety Document Manual. [2.25]

**Acquired Software**

- Commercial grade software that will be qualified by SRS prior to being placed in service for its intended use in accordance with E7, Section 5.0 or QAP 20-1.
- Software that will be developed and qualified by a supplier in accordance with E7 Section 5.0 or QAP 20-1. [5.07]

**Administrative Controls** – see WSRC Manual 11Q, Facility Safety Document Manual. [2.25]

**ALARA** - an acronym for the concept of reducing radiation dose to levels As Low As Reasonably Achievable. ALARA is not a dose limit but constitutes a design philosophy that promotes the optimizing of design for keeping radiation doses to personnel as far below the applicable limits as social, technical, economic, practical and public policy considerations reasonably permit. [2.72]

**Alternate Replacement Item** - A replacement item not "like-for-like" to the original item, (i.e., it does not match the form, fit, and function of the item being replaced), however, it must fulfill the required safety functions. Alternate Replacement Items require a formal (documented) evaluation to ensure the safety functions will be maintained. Documentation of the evaluation is performed via a Design Change Package (DCP)/Design Change Form (DCF), when the item is part of the controlled Technical Baseline. If desired, additional evaluation may be documented using the Replacement Item Evaluation (RIE) form (OSR 19-341). [3.46]

**Alternatives Study** - an evaluation of alternatives to select the one that best meets the physical, functional, and operational requirements. [2.15]

**Annual Operating Plan** - the formal agreement of work scope, schedule (milestone), resources, and budgeted costs between WSRC and DOE that is summarized, documented, and authorized. [2.02]

**Anticipated** - frequency that is greater than or equal to 10-2 per year and less than 1. [2.25]

**Approval Date** - the date a procedure is signed by the approval authority and approved for use. [1.01]

**Area** - the site area code identifies the physical area of the site to

which the component applies. [1.30]

**As-Built Drawing** - a record drawing that reflects the existing or as-installed configuration of structures, systems, or components within specified design tolerances defined by codes, standards, or project requirements. [1.53]

**Assembly** - a combination of subassemblies, components or both which form a workable unit (e.g., control room panels, motor control centers, skid mounted equipment, etc.). [3.46]

**Assessment Package** - document used to record the evaluation of adequacy for a given SSC or group of similar SSCs to perform an identified function relative to the applicable design criteria. [3.41]

**Assessment/Verification** – see WSRC 1Q, Quality Assurance Manual. [2.31]

**Authenticator** – The person who performs authentication as defined in WSRC Manual 1B. [2.30]

**Authorization Basis (AB)** – see WSRC Manual 11Q, Facility Safety Document Manual. [3.41]

**Backfit Analysis** - the process by which an existing SSC is evaluated to determine if it is adequate to perform its upgraded safety function in terms of newly-established requirements and safety analyses. Backfit consists of a design assessment and if needed a cost benefit assessment. These activities are conducted by the Backfit Assessment Team and the results are reviewed and approved by an Engineering Review Board. [3.41]

**Baseline** - A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for use and further development, and that can be changed only by using an approved change control process. [5.61]

**Baseline Operating Data (BOD)** – a "non-critical" pre-defined qualitative or quantitative observation or data collection that does not require testing ranges or tolerances to satisfy a performance requirement. Values/data collected are identified as “expected” values and are used to evaluate data/system performance. [2.26]

**Beyond Extremely Unlikely (BEU)** - a frequency of occurrence that



is conservatively estimated to be less than  $10^{-6}$  per year. [2.25]

**Boundary** - defines locations of all physical interfaces of an SSC. It specifically identifies the points where these SSCs interface with the SSC being bounded. [1.05]

**Bounding Conditions** - parameters that envelop the normal, abnormal and accident environmental conditions an item is expected to meet during its lifetime in the facility (e.g., temperature, humidity, radiation, seismic response spectra, etc.) [3.46]

**Certification** – see WSRC Manual 1Q, Glossary. [3.46]

**Challenge** – To come close to or exceed the Safety Class or Safety Significant criteria. [2.25]

**Characteristics** – Any property or attribute of an item, process, or service that is distinct, describable, and measurable. [3.46]

**Closure** – the act of integrating into the baseline an implemented and accepted modification. [5.62]

**Cloud** - a method of identifying changes on a document by enclosing them with a scalloped line. [1.57]

**Code of Record (COR)** – see WSRC-TM-95-1, Engineering Standards Program Roles and Responsibilities. [3.41]

**Commercial Design Checking** - the process by which an engineering document is evaluated for accuracy against specific requirements. Indication of satisfactory completion of design checking is provided directly on the document that is checked. [1.56]

**Commercial Engineering Calculation** - a written record documenting an analytical or computational thought process used to support an engineering justification or to support the design or operation of a structure, system, or component. Commercial engineering calculations are defined as either type 1 commercial, type 2 commercial, or informal. [1.54]

**Commercial Grade Item (CGI)** - When used in a Safety application (SS/SC), an item is a CGI when it satisfies all three of the following criteria:

1. Not subject to design or specification requirements that are unique to SRS nuclear facilities;
2. Routinely used in applications other than SRS nuclear facilities, and
3. Is to be ordered from the manufacturer/supplier on the basis of specifications set forth in the manufacturer's published product description (for example, a catalog). [3.46]

**Commercial Grade Survey (Verification Method 2)** - activities conducted by WSRC or its agent to verify that a supplier of commercial grade items controls, through quality activities, the critical characteristics of specifically designated commercial grade item, as a method to accept those items for safety use. [3.46]

**Commercial Technical Review** - an evaluation of an engineering activity for technical adequacy, impact on safety, operations, maintenance, and the technical baseline. [1.58]

**Commodity Item** - an item having a generic application throughout a nuclear facility, which lends itself to bulk procurement (e.g., nuts, bolts, materials, O-rings, gaskets, indicator lights, fuses, relays, resistors, etc.).

**Competent Authority (Type B and Type A packaging)** – a national agency responsible under national law for the control or regulation of a particular aspect of the transportation of hazardous materials offsite. [4.05]

**Component** – a part or assembly of parts viewed as a functional entity within a system for purposes of providing a unique function within a system (e.g., pumps and valves) and that is identified by a unique identifier, e.g., Component Location Identifier (CLI). [1.30]

**Component Number** - a alpha-numeric identifier assigned to a component or unit of equipment to uniquely identify that component or unit of equipment. Component and equipment numbers are also known as Component/Process Location Identifier (C/PLI), Component Location Identifier (CLI) and Process Location Identifier (PLI). [1.30]

**Computer Program** - A combination of computer instructions and data definitions that enables computer hardware to perform computational or control functions. [5.61]

**Computer Program Error** - A condition of a computer program producing incorrect results or a condition deviating from an established baseline, including deviations from the current approved computer program and its baseline requirements. [5.61]

**Computer Program Modification Tracker (CMT)** – a system used to track, from approval to closure, a modification to baseline software (computer program file or associated document) identified as a Configuration Item in a Software Quality Assurance Plan. [5.62]

**Configuration** - the functional, physical, and operational characteristics of a structure, system, or component as defined in its technical baseline. [1.05]

**Configuration Control** - the integrated, systematic process to propose, coordinate, evaluate, and disposition changes in order to assure that each configuration change provides sufficient benefits for its impacts and consistency between a SSC's requirements, its technical baseline and the actual SSC is maintained. [1.05]

**Configuration Controlled SSC** – an SSC that meets the criteria for a CLI in accordance with procedure 1.30, Manual E7. [1.02]

**Configuration Item (CI)** – Hardware or software elements treated as a unit for the purpose of configuration control. Refer to Manual 1Q, QAP 20-1. [5.62]

**Configuration Management** – an integrated process that establishes accuracy and consistency among design requirements, physical configuration, and facility documentation, and maintains this consistency throughout the life of the facility. CM consists of the following program elements: program management, design requirements, document control, change control and assessments. (DOE-STD-1073-93)

**Confirmatory Test** - a test performed to obtain corroborating data for all or part of the range of one or more parameters included in a non-qualified data set. [3.70]

**Conforming ID** - a component number that conforms to this procedure. [1.30]

**Consequence of Occurrence (C)** - see [WSRC-IM-98-00033](#),

## Appendix B.

**Corroborating Data** - data that is used to help establish the technical credibility of non-qualified data. Corroborating data may include information developed from records searches, records of field walkdowns, design document reviews, and records of interviews with subject matter experts. [3.70]

**Credible Event** - an event which is more frequent than Beyond Extremely Unlikely. [2.25]

**Credible Failure Mechanism**- the credible manner by which an item may fail, degrading the item's ability to perform the component/system function under evaluation. This determination also considers mitigating factors (preventive maintenance, surveillance testing, etc.) which may prevent the failure from occurring. [3.46]

**Critical Characteristics for Acceptance (CCFA)** – Those properties or attributes of a CGI which, once selected and verified, provide reasonable assurance that the item will perform its intended safety function. An item's CCFAs may be a combination of design characteristics, along with other item characteristics. [3.46]

**Critical Spare Equipment** – Specific serialized items requiring identification, maintenance and storage in support of plant operations. These items are identified as a UTC in Passport. [1.31]

**Data** – a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. [5.80]

**Data Dictionary** – a collection of entries specifying the name, source, usage, and format of each data element used in a system or set of systems. [5.80]

**Data Element** – (1) a uniquely named and defined component of a data definition; a data "cell" into which data items (actual values) can be placed. For example, the data element AGE, into which data items 1, 2... can be placed. Note: The terms data element and data item are often used interchangeably or with the reverse definitions from those given here. No standard of use exists at this time. Syn: cell. (2) a data definition as in (1) that cannot be divided into other individually

named data definitions. [5.80]

**Data Item** – a value contained in a data element. [5.80]

**Data Management Plan (DMP)** – the document for controlling data management activities by defining the administrative processes used to create, modify, and maintain data. [5.80]

**Data Modification Tracker (DMT)** – paper or electronic form used for processing a data modification request. [5.80]

**Data Set** – a named collection of related records (often synonymous with file). [5.80]

**Dedication** - A process undertaken to provide reasonable assurance that a Commercial Grade Item (CGI) to be used in a safety (SS/SC) application will perform its intended safety function and in this respect, it is deemed equivalent to an item designed and manufactured under the WSRC QA program. [3.46]

**Defense in Depth** – Defense in Depth refers to the broad-based layers of protection against uncontrolled releases of Hazardous Material to the environment. It is based on multiple layers of defense against release of Hazardous Materials so that no one layer by itself, no matter how good, is completely relied upon. This compensates for potential human and mechanical failures. [2.25]

**Design Adequacy Assessment** – the process of comparing a proposed SSCs design to a set of design criteria and qualitatively or quantitatively justifying acceptability of design if any applicable criteria are not met. [3.41]

**Design Agency** - a Technical Agency assigned by the Modification Manager to perform a software modification or the detailed design and analysis activities of a plant modification. [2.05]

**Design Authority** - the person or group responsible for the final acceptability of, and changes to, the design of software and its baseline or a structure, system or component and its technical baseline. [1.10]

**Design Authority Engineer** - the person within the Design Authority organization that is assigned Design Authority responsibility. The Design Authority Engineer has review and

approval authority for modifications to assigned structures, systems and components. [1.10]

**Design Authority Technical Review** - an evaluation of a modification for technical acceptability, impacts on safety, operation and maintenance, and impacts on the Authorization Basis. [3.14]

**Design Change Form (DCF)** - a form used to request, document, and process a change to a technical baseline document after its release for use. [2.37]

**Design Change Notice (DCN)** - a form used as part of a DCP to request, document, and process changes to existing drawings, quality inspection plans, specifications, and vendor documents. [2.38]

**Design Change Package (DCP)** - a package consisting of approved interim design documents, required instructions and specifications, the identification of prerequisite projects or tasks, and other documents required to implement and properly record a specifically defined design change. [2.38]

**Design Checking** - the process by which an engineering document is evaluated for accuracy against specific requirements. Documentation of this review is provided directly on the document that is checked. [2.40]

**Design Consistency** – a process to design systems within a facility or division such that similar or duplicate systems (i.e., multiple chiller units) are designed to be operated under the same procedure and maintained with a common set of spares. [2.05]

**Design Document for Software (DDS)** – the controlling document that specifies the design of a software product. [5.20]

**Design Freeze** - the point, determined by the Design Authority, at which changes to the project design require more control and approval than is afforded by a Design Change Form (i.e., a DCP is required). This is normally in anticipation of start up or turnover to operations. [2.38]

**Design Function** - the operation an item is required to perform to meet the component or system design basis. [3.46]

**Design Verification** - the act of reviewing, testing, or otherwise

determining and documenting whether the technical baseline (including DSA calculations) of a structure, system, or component meets specified requirements. [2.40]

**Development Drawing** - a drawing that is created and controlled entirely within a Technical Agency for use in the design, procurement, construction, fabrication, or installation of systems or components that are not part of a facility technical baseline. [2.30]

**Development Program Manager** – the Technical Agency point-of-contact assigned lead responsibility for technology development activities. [2.07]

**Division Managed Modification** - Modification funded from operating expense. [1.02]

**Direct Effect** – The output of the software is used in the operation of an SSC with no additional evaluation or review prior to taking action. [5.05]

**Direct Revision** - the process of revising a controlled document by directly changing the text or pictorial information without the use of any additional change paper. [1.53]

**Disposition** - the direct result or conclusion of a Technical Assistance Request. The preliminary disposition contains the conclusions that were reached, sets the schedule for, and summarizes the path forward for, the concluding disposition. The Technical Assistance Request is considered closed at the concluding disposition. [3.12]

**Document** - recorded information that describes, specifies, reports, certifies, requires, or provides data or results. For the purpose of the CM program, this includes paper copies (procedure, manuals, records, etc.), electronic media (such as word processor files and computer databases), and any other source(s) of information used to design or operate the facility or make sound technical decisions. It includes both current or working documents and historical records. [1.05]

**Documented Safety Analysis (DSA)** – See WSRC Manual 11Q, Facility Safety Document Manual. [2.25]

**Effective Date** - the date that affected organizations are accountable

to be in full compliance with the procedure including completion of all required training. [1.01]

**Engineering and Scientific Software** - Software that produces results that are used by engineering organizations in, or in support of, SRS technical documents. [5.61]

**Engineering Calculation** - a written record documenting an analytical or computational thought process used to support an engineering justification or to support the design or operation of a structure, system, or component. Engineering calculations are defined as either type 1 or type 2 calculations. [2.31]

**Engineering Calculation Software** - the computer programs, procedures, rules, and associated documentation and data pertaining to performing Engineering Calculations using a computer or programmable device. This software includes, but is not limited to, software used in programmable devices such as calculators, purchased (e.g., MATHCAD, EXCEL, etc.) or Site developed software, software layers, macros, routines, operating parameters, and data tables. The data referred to in this definition do not include the input and output data for the subject calculation. [2.31]

**Engineering Document** - design input, design output, and related documentation generated in support of a new structure, system, or component (SSC) or to support a plant modification. [1.20]

**Engineering Document Number** - a combination of alpha and numeric characters that uniquely identify an individual engineering document. [1.20]

**Engineering Review Board (ERB)** - the Engineering Review Board provides an oversight and approval function for Backfit Analysis activities. Membership is limited, and members will be selected by the Division Chief Engineer based on overall experience, skill mix needs, and facility familiarity. In the event that a Backfit Analysis involves more than one facility, all facilities impacted by the analysis will be represented on the ERB. The ERB is responsible for reviewing and approving the Backfit Analysis package. [3.41]

**Equipment** – An engineered item that includes characteristics or salient features based on conditions and operating parameters of a facility. Equipment includes items such as pumps, motors, tanks,



valves, instruments, panels, etc. used for facility operation. [1.30]

**Equivalency Evaluation** - a technical evaluation performed to confirm that an alternative item, not like-for-like to the original or installed item, will satisfactorily perform its intended function once in service. This term is synonymous with "Equal-to-or-Better-Than Evaluation." [3.46]

**Equivalent Safety** – See WSRC Manual 19Q, Transportation Safety [4.06]

**Essential Comment** – Comment that requires resolution. [1.01]

**Essential Document** - document type that (1) demonstrates that the SSCs addressed by the authorization basis will perform their active safety function and (2) is used by engineering and operations to quickly respond to plant events. [1.05]

**Evaluation Guideline (EG)** – Public hazardous material dose/exposure value that the safety analysis is evaluated against. [2.25]

**Existing Software** – Software that has been developed using an engineering methodology that is not in accordance with E7, Section 5.0, or a quality program that is not in accordance with QAP 20-1. [5.07]

**Extremely Unlikely** - frequency which is greater than or equal to  $10^{-6}$  per year and less than  $10^{-4}$  per year. [2.25]

**Facilities** – land, buildings and other structures, their functional systems and equipment, and other fixed systems and equipment installed therein including site development features outside the plant, such as landscaping, roads, walks, and parking areas; outside lighting and communications systems; central utility plants; utilities supply and distribution systems; and other physical plant features. [2.12]

**Facility Design Description (FDD)** - the facility technical document that defines the top-level functions, performance, design, physical, testing, interface, operating, and maintenance requirements for a facility. The FDD provides the single source for communicating and controlling the facility level requirements. [2.12]

**Facility Technical Baseline** - all technical baseline documents under the control of a facility Design Authority. [2.37]

**Failure Modes and Effects Analysis** - an evaluation of credible failure mechanisms and their effect on system/component function. [3.46]

**Failure Mode** - the effects or conditions which result from an item's credible failure mechanisms. [3.46]

**Federal Facilities Agreement (FFA)** - the agreement signed by the Environmental Protection Agency (EPA), South Carolina Department of Health and Environmental Control (SCDHEC), and United States Department of Energy (DOE) that regulates the site waste remediation process and integrates the requirements of the Comprehensive Emergency Response, Compensation, and Liability Act (CERCLA) and the Resource Conservation and Recovery Act (RCRA). [1.40]

**Feasibility Study** - an evaluation of a proposed plant modification performed to aid in determining the scope and functional requirements of the modification. A feasibility study may include a technology assessment. [1.02]

**Field Change Request (FCR)** - an engineering design document used to request and process a change to an issued engineering document. [1.55]

**Field Sketches** - a drawing created in conjunction with design output documents to assist in the fabrication or installation of structures, systems, or components, or a drawing used for maintenance or modification instructions to ensure clear direction. [2.30]

**Final Inspection** - inspections that are typically performed during the initial installation or major modification of items/systems up to and including tests performed prior to facility operation. An inspection is considered final when it addresses all inspections required within the scope of a work package or completes inspections within the scope of a work package that were not previously completed in-process. (Ref. 1Q Glossary) [2.36]

**Final Documented Safety Analysis** – Safety Analysis that meets 10 CFR 830 requirements and DOE-STD-3009-94 guidance or a WSRC

approved Documented safety Analysis that is considered by DOE to fulfill the commitments made in the standards/Requirements Identification Documents (S/RID) as documented in the Compliance Assessment and Implementation Report for 10 CFR 830.

**Final Safety Analysis** - Safety Analysis that meets DOE Order 5480.23 requirements and DOE-STD-3009-94 guidance or a WSRC approved Authorization Basis that is considered by DOE to fulfill the commitments made in the standards/Requirements Identification Documents (SRID) as documented in the Compliance Assessment and Implementation Report for DOE Order 5480.23. [2.25]

**First-Time Use** – See WSRC Manual 19Q, Transportation Safety [3.15]

**First-Time Use technical review** – See WSRC Manual 19Q, Transportation Safety [3.15]

**Fit** - those characteristics of an item that define the location and connection of installation interfaces (e.g., dimensions, matchup, and method of mounting). [3.46]

**Form** - those characteristics of an item that define the physical envelope (e.g., type or style of item, weight, material composition, and dimensional shape). [3.46]

**Formal Design Review** - an independent assessment of the technical adequacy of selected portions of the plant modification task input documents and an independent assessment for compliance of task output documents with the plant modification requirements in the task input documents. [2.65]

**Formal Design Review Board (Board)** - the selected group of individuals that shall review and comment on the Data Package submitted for Formal Design Review. [2.65]

**Formal Design Review Data Package (Data Package)** - Formal Design Review information that includes the approved task input documents and task output documents and normally any supporting analytical and test results for a plant modification under review. The data package may include the results of the Technical Risk Analysis. [2.65]

**Formal Design Review Methodology Manual** - procedure

implementation information containing detailed supplementary material intended to assist all participants to hold effective Formal Design Reviews consistent with the intent of this procedure. [2.65]

**Function** - the operation an item is required to perform to meet the component or system design basis. [3.46]

**Functional Acceptance Criteria** - a measurable set of characteristics used to define the acceptable performance that satisfies a functional requirement(s). This is used as the input to the Manual 5E process. Functional Acceptance Criteria Documents are written to the level of system performance characteristics, so that acceptance tests can be developed. [2.26]

**Functions and Requirements** – those performance criteria and design constraints which the structure, system, or component must meet in order to be acceptable. [2.15]

**Functional Acceptance Criteria (FAC)** – a measurable set of characteristics used to define the acceptable performance that satisfies a testable performance requirement. FAC are written to the level of system performance characteristics, so that tests can be developed. TAC, GTD, and BOD are specified from FAC. [2.26]

**Functional Classification** - a graded classification system used to determine minimum requirements for SSCs (i.e., design, operation, procurement, and maintenance requirements). The four Functional Classifications in order of precedence are Safety Class, Safety Significant, Production Support, and General Services. There are three possible statuses for a Functional Classification; Preliminary, Interim and Final. The status is the same as the status of the Safety Analysis used to determine the classification. The statuses preliminary and interim apply only to Safety Class and Safety Significant classifications. Production Support and General Services classifications are based on information that is independent of the Safety Analysis status and may always be considered final. [2.25]

**Functional Mode** - the functional mode of a component is determined to be either active or passive based on the definitions of those terms given in WSRC-TM-93-9. [2.25]

**General Document** - document types that provide engineering details necessary for construction and are updated at the discretion of

the Design Authority. [1.05]

**General Services** - the functional classification assigned to all SSCs not required to provide a Safety Class, Safety Significant, or Production Support function. All SRS SSCs are, as a minimum, classified as General Services to assure that proper design, operations, and maintenance requirements are assigned to provide for the health and safety of the worker and environment and to assure compliance with other Site requirements. [2.25]

**General Test Data (GTD)** – a "non-critical" pre-defined qualitative or quantitative measurement that requires testing to verify a performance requirement. [2.26]

**Graded Approach** - a process by which the level of analysis, documentation, and actions necessary to comply with a requirement are made commensurate with a number of considerations, including the relative importance to safety, safeguards, and security; the magnitude of any hazard involved; the life cycle stage of a facility; the programmatic mission of a facility; the particular characteristics of a facility; and any other relevant factor. (DOE-STD-1073-93)

**Grassroot Modification** – a modification which adds a new system or facility not in the control of, or critical to, operations and where the modification does not impact existing facilities except for the points of interface. Grassroot modification points of interface with existing facilities are controlled as Plant Modifications. [2.30]

**Hazard** – see WSRC Manual 11Q, Facility Safety Document Manual. [2.25]

**Hazard Analysis** – see WSRC Manual 11Q, Facility Safety Document Manual. [2.25]

**Hazardous Material** - any solid, liquid, or gaseous material that is toxic, explosive, flammable, corrosive, or otherwise physically or biologically threatening to health. [Candidate Hazards as used in this procedure include radioactive materials and hazardous chemicals that are not common Hazardous Material as defined in the EMPP 6Q-001, Manual 6Q.] [2.25]

**Hold Point** - a mandatory inspection activity beyond which work shall not proceed until 1) inspection is performed and acceptance is

authenticated; or 2) written release is authorized by Engineering. [2.36]

**Human Factors Engineering (HFE)** - the application of information about human behavior, abilities and limitations in the design process to ensure safe, comfortable, and effective use of HSIs. [2.18]

**Human Factors Engineering Plan (HFEP)** - the governing document for the HFE engineering process that describes the HFE requirements and responsibilities, tailored for facilities, systems or projects (applying a graded approach). [2.18]

**Human-System Interface (HSI)** - a point of interaction between personnel and equipment (displays, computers, alarms, controls, decision aids, workstations, communication devices, and environments) where the resulting human performance impacts system performance. [2.18]

**Implementing Agency** - the organization assigned to implement the physical work associated with the plant modification or implementation activities associated with the software modification (translation of design into code). [2.38]

**Independent Inspection** - examination or measurement to verify whether an item or activity conforms to specified requirements; performed by an individual who is qualified and certified in accordance with Procedure Manual 1Q, Quality Assurance Manual, Procedure 2-5, "Training, Qualification and Certification of Inspection Personnel", and Procedure 10-1, "Inspection"; and, who did not accomplish the task to be inspected and was not involved in the performance of the activity. [2.36]

**Independent Review** - There are two types of Independent Reviews: Type 1 and Type 2. A Type 1 Independent Review (IR-1) is the review of a document performed by an individual knowledgeable in the area of review to ensure that the assumptions, methodology and resulting product reflect sound engineering judgment. An individual other than the individual that did the work being reviewed conducts the Independent Review. A Type 2 Independent Review (IR-2) is similar to an IR-1 with the added requirement that it be conducted by an individual subject to a different technical direction (i.e., not

assigned to the same project or task). [5.03]

**Indirect Effect** – The output of software is used in the operation of an SSC but is subject to evaluation or review prior to taking action. [5.05]

**Individual Review of Calculation** - Review performed by an individual other than the calculation preparer to evaluate technical adequacy of the calculation approach, ensure internal completeness, consistency, clarity and correctness of arithmetic, and verify the assumptions are traceable to the requirements. [2.31]

**Industrial Modifications** - Modifications outside a nuclear facility and their safety support facilities (WSRC-RP-94-1268) to GS and PS SSCs which are involved in operations in which material is chemically or physically transformed from one state into another and/or pose a significant risk to personnel safety. This definition includes chemical operations, handling/transportation of hazardous materials, power and water distribution systems, power/steam production, and fire protection. [1.02]

**Informal Calculation** - a calculation supporting engineering designs having no significant technical, safety, or economic risk. Informal calculations use a graded approach toward technical and computational detail and are controlled internally and maintained within engineering files. [1.54]

**Infrastructure Modifications** - Modifications outside a nuclear facility and their safety support facilities (WSRC-RP-94-1268) to GS and PS SSCs that are not part of an Industrial Modification. This definition includes roads, railroads, bridges, structures (including administrative buildings and warehouses), telecommunications, dams, landfills and similar items. [1.02]

**In-Process Inspection** - inspections that are typically performed during the initial installation or major modification of items/systems up to and including tests performed prior to facility operation. An inspection is considered in-process when it is performed, completed, and the reporting document is reviewed and closed prior to all inspections within the scope of a work package being complete. (Ref. 1Q Glossary) [2.36]

**Inspection** - examination or measurement to verify whether an item



or activity conforms to specified requirements. [2.36]

**Install** - placement/securing of equipment, conductor or conduit/piping per design prior to being energized. [3.80]

**Integrated Safety Management System (ISMS)**, Tailored Approach To - The practice of specifying requirements, design attributes, and operating strategies that result in safe and successful DOE mission accomplishment at minimum cost.

**Interim Drawing** – a drawing issued to support a Design Change Package (DCP) and issued as part of the DCP. [2.30]

**Interim Safety Analysis** - an existing facility, DOE approved safety documentation scheduled (with DOE concurrence) for replacement. These are not considered by DOE to fulfill the commitments made in the SRIDs as documented in the Compliance Assessment and Implementation Report for 10 CFR 830. [2.25]

**Item** - An all-inclusive term used in place of any of the following: appurtenance, assembly, component, equipment, material, module, part, software, structure, subassembly, subsystem, system, or unit.

**Justification for Continued Operation (JCO) /Technical Justification for Continued Operation (TJCO)**– see WSRC Facility Safety Document Manual 11Q [3.41]

**Lay-up Modification** - modifications performed on structures, systems, or components that have been removed from service to accomplish activities such as:

- protecting them from degradation in accordance with a facility or system lay-up plan, or
- providing for running of equipment outside normal operating configuration to support lay-up, partial shutdown, or complete shutdown.

Lay-up modifications are not permanent plant modifications. Lay-up modifications cannot be left in place during normal system operation. [2.06]

**Lay-up Plan** – a plan prepared for the preservation of equipment and systems to be removed from service for an extended period of time. [2.06]



**Level A** - See WSRC Manual 1Q, [QAP 20-1](#). [5.05]

**Level B** – See WSRC Manual 1Q, QAP 20-1. [5.05]

**Level C** – See WSRC Manual 1Q, QAP 20-1. [5.05]

**Level D** - See WSRC Manual 1Q, QAP 20-1. [5.05]

**Level E** - See WSRC Manual 1Q, QAP 20-1. [5.05]

**Level of Control (LOC)**- one or more structures, systems, components, administrative controls, or inherent features (e.g., chemical properties, gravity, physical constants, underground location) that can be readily expected to act to Prevent or Mitigate the release of Hazardous Material to an unwanted location. [2.25]

**Like-for-Like Item** - An item having the same form, fit and function attributes as the item it replaces. "Identical" items (same make, model number, characteristics, etc., as determined by being obtained via the same purchase order) are a subset of like-for-like items.

**Master Equipment List (MEL)** – A detailed listing of SSCs, special tools, and critical spare equipment contained in the Site Work Management System (Passport). [1.31]

**Metadata** – data that describes other data; for example, a data dictionary contains a collection of metadata. [5.80]

**Minor Modification** - facility modification that meets the following conditions as further defined by the operating division: [1.02]

- relatively low cost
- does not require significant or long term commitments of engineering, crafts, or work control
- has few or no discipline interfaces
- is simple to implement and is an obvious solution to a specific problem
- does not involve an unreviewed safety question
- does not impact the design basis of the Structure, System, or Component (SSC) being modified
- involves few document changes

**Mitigate** - to lessen the severity of consequences of an event. [2.25]

**Mitigated** –taking credit for preventors and/or mitigators. [ 2.25]

**Modification** - a physical change to a configuration controlled Structure, System or Component (SSC). Modifications include new facilities, and additions, deletions or changes to existing facilities

[1.02]

**Modification Manager** - person designated by the Design Authority to have overall responsibility for a plant modification. [2.05]

**Modification Team** - team, comprised of members from the operating division, Projects Engineering and Construction Division (PE&CD), and supporting organizations, led by the project manager and with total responsibility for all aspects of the development and execution of assigned modifications.

**Modification Traveler (MT)** - a document or electronic system used to track a modification from initiation to closure and may be used to document and control design input requirements and criteria. [2.05]

**Monitored Parameters** - a measurable characteristic of a system or component that provides information (e.g., flow, temperature, pressure) to evaluate the performance of a system or component. [3.04]

**New Application** – software that has not yet been baselined, is a new deployment of existing software or has been specifically developed to meet new requirements. [5.01]

**New Information (NI)** - see WSRC Facility Safety Document Manual 11Q [3.41]

**Non-conforming ID** - a component number that does not conform to this procedure. Such IDs are those component numbers that were derived by procedures that existed prior to this procedure (legacy IDs). [1.30]

**Non-Essential Comment** – Comment that is incorporated at the discretion of the E7 Manual Coordinator. [1.01]

**Non-Facility Based SSCs** - SSCs (or items) that cannot be associated with a SRS facility and functionally classified in accordance with Manual E7, Procedure 2.25 (e.g. standard waste boxes and 55 gallon storage drums). [3.10]

**Non-qualified Data** - data for which documentation may not exist to demonstrate their compliance with current QA or procedural requirements. [3.70]

**Non-Technical Baseline (NTB)** - Reference documentation (drawings, etc.) related to facility SSCs but not included in the Facility's Technical Baseline as defined by E7, 1.05 (i.e., not configuration controlled). [1.20]

**Nuclear Facility** – see WSRC Manual 11Q, Facility Safety Document Manual. [2.25]

**Nuclear Production Facility** - a facility whose primary mission is to analyze, produce, process, or store nuclear materials. [2.25]

**Offsite shipment** - See WSRC Manual 19Q, Transportation Safety [4.05]

**Onsite In-Commerce (OSIC)** – See WSRC Manual 19Q, Transportation Safety [4.06]

**Onsite Package Authorization Form (OPAF)** – See WSRC Manual 19Q, Transportation Safety [4.06]

**Onsite Safety Evaluation Review (OSER)** - See WSRC Manual 19Q, Transportation Safety [4.06]

**Onsite Safety Assessment (OSA)** - See WSRC Manual 19Q, Transportation Safety [4.06]

**Onsite transfer** – See WSRC Manual 19Q, Transportation Safety [4.06]

**Open Items** - unconfirmed or unchecked input, assumptions, or results that must be verified. A type 1 calculation containing open items is either a preliminary calculation or committed calculation and may not be designated as confirmed until all open items are closed. [2.31]

**Package** - See WSRC Manual 19Q, Transportation Safety [3.15]

**Package Authorization**– the summary approval document based on a graded technical safety evaluation consistent with the associated hazard and issued by an authority commensurate with the associated hazards. These include:

- DOE, NRC or IAEA Certificate of Compliance.
- Onsite Package Authorization Form

- Type A Package approval documentation
- Industrial package documentation
- Strong-Tight container documentation [3.15]

**Package Contents** – anything that is loaded into the packaging that is not part of the packaging [3.15]

**Packaging (radioactive)** - See WSRC Manual 19Q, Transportation Safety [3.15]

**Part** - items from which a component is assembled (e.g., resistors, capacitors, wires, connectors, transistors, lubricants, O-rings, springs, bearings, gaskets, bolting, seals, etc.). [3.46]

**Part Number** -an identifier assigned by a supplier for a commercial grade item. Part number as used herein can also include identifiers such as model number, material type, grade, catalog reference number, etc. [3.46]

**Peer Inspection** - examination or measurement to verify whether an item or activity conforms to specified requirements; performed by an individual who is task and inspection qualified in accordance with Procedure Manual 1Q, Quality Assurance Manual, Procedure 10-1, “Inspection”; and, who did not accomplish the task to be inspected, but, may have been involved in the performance of the work activity. [2.36]

**Performance-Based Specification** – a statement of requirements in terms of required results with criteria for verifying compliance, without stating methods for achieving the required results. [2.14]

**Performance Monitoring** - systematic review, recording, and trending of monitored parameters of systems and components to measure and assess the impact of any performance changes of a particular system or component. [3.04]

**Performance Requirement** – a criteria that must be verified by analysis, inspection, review, or testing to demonstrate acceptable technical performance of a plant modification. [2.26]

**Performing Entity** – The companies comprised of Westinghouse Savannah River Company, Bechtel Savannah River, Inc., BWXT Savannah River Company, BNFL Savannah River Corporation, CH2

Savannah River Company, etc.

**Physical, Functional, and Operational Requirements** - those characteristics against which the structure, system, or component will be evaluated to determine acceptability. [2.15]

**Plant Event** - an unplanned, abnormal event that occurs during normal plant operations. [1.05]

**Plant Modification** - the addition, deletion, or change to the configuration of a configuration controlled SSC and its technical baseline. A plant modification will always include a technical baseline modification and a physical modification. [2.05]

**Plant Modification Technical Baseline** - all technical baseline documents generated for structures, systems, and components as part of a plant modification. [2.37]

**Plant Modification Technical Review** - an independent evaluation for compliance of the technical baseline task output with the technical baseline task input and an evaluation of the technical adequacy of selected portions of the technical baseline task output. The three types of Plant Modification Technical Reviews are Formal Design Review (FDR), Design Authority Technical Review (DATR), and Design Verification by Interdisciplinary Evaluation (DVIE). [2.60]

**Pollution Prevention (P2)** - the use of any process, practice, or product that reduces or eliminates the generation and release of pollutants, contaminants, hazardous substances, and wastes into all environmental media including ground, water, and air and/or conserves natural resources, including energy conservation. Within DOE, pollution prevention includes all aspects of source reduction as defined by the U.S. Environmental Protection Agency (EPA) in the Pollution Prevention Act and incorporates waste minimization by expanding beyond the EPA definition of Pollution Prevention to include recycling. [1.41]

**Pollution Prevention in Design (P2D)** - a process of designing for pollution prevention to minimize raw material consumption, energy consumption, waste generation, health and safety impacts, and ecological degradation over the entire life of the facility. [1.41]

**Pollution Prevention Design Assessment (P2DA)** - a Pollution Prevention Opportunity Assessment conducted during the design phase of the new products, processes, and facilities. [1.41]

**Pollution Prevention Design Opportunity (P2DO)** - specific design changes that would prevent or minimize the anticipated waste streams. [1.41]

**Pollution Prevention Opportunity Assessment (PPOA)** - a review of an operation, process, activity, or waste/pollution stream with the objective of identifying and evaluating ways to eliminate or reduce waste/pollution and/or conserve natural resources. [1.41]

**Post-Installation Tests/Post-Maintenance Tests (included in Verification Method 1)** - activities conducted after installation of a commercial grade item to verify required critical characteristics prior to placement in operation. An element of the "Special Tests and Inspection" method to accept an item for safety use. When specific post-installation acceptance criteria are specified in a RICP or CGD, a Post-Installation Test (PIT) is hung on the item to identify that one or more additional dedication activities remain to be performed. When the post-installation acceptance criteria are specified in the Work Package, the test is referred to as a Post-Maintenance Test (PMT) and the PIT tag is not hung on the item. [3.46]

**Power Services** - plant systems that provide steam, electricity, domestic water, process water, or sanitary waste treatment. [3.80]

**Power Services Utilization Permits (PSUPs) Parts A, B, and C** – a form used to document the request for changes to power services (Parts A and B) and to document verification and adequacy of protective devices for site electrical systems (Part C). [3.80]

**Preliminary Safety Analysis** - the safety analyses performed during the development of the design of a plant modification or new facility. [2.25]

**Prevent** - to lessen the frequency of an event. [2.25]

**Primary Documentation** - documentation consisting of the technical baseline, memoranda, laboratory notebooks, or other documents that are used to support the analyses or conclusions contained in a technical report. [3.60]

**Probability of Occurrence (P)** - see [WSRC-IM-98-00033](#), Appendix B.

**Process Software** – Software that is functionally classified as part of an SSC. [5.05]

**Procurement Quality Requirement** - those necessary and sufficient measures identified to ensure that the deliverables in a procurement activity will be provided in accordance with the technical and supplemental requirements specified in the procurement documentation. Procurement Quality Requirements are derived from and aligned with the technical requirements generated by the Responsible Engineer, and are applied on a graded approach commensurate with the functional and technical requirements. (3E). [3.10]

**Production Support** - the Functional Classification that applies to those SSCs necessary to support continued operation of a Nuclear Production Facility and to selected environmental monitoring and Emergency Plan communications devices. [2.25]

**Professional Engineer Certification** - the statement of responsibility, seal and signature applied by the Registered Professional Engineer on any document. [1.40]

**Project Team** - all SRS employees who perform work under the direction of the Project Manager or designee. [2.65]

**Public** - population outside the SRS boundary at the time of the event. [2.25]

**Quality Inspection Plan (QIP)** - a document that uniquely identifies, on a plant modification basis, the inspection and test requirements, acceptance criteria, and responsibilities of the Implementing Agency for items and actions identified in the Quality Assessment Report. QIPs may also be used for specifying additional inspection or test requirements identified by the Design Agency to verify that specified design requirements have been satisfied. [2.36]

**Quality Requirement** - a characteristic that must be present for a structure, system, or component to function safely and effectively in its intended operating environment. [2.36]

**Radioactive Material** – See WSRC Manual 19Q, Transportation

Safety [3.15]

**"Ready for Formal Design Review" Memo** - documentation from the Design Team Leader verifying selected task input and output documents are ready for a Formal Design Review and is issued to the Formal Design Review Coordinator and Board. [2.65]

**Receiving Inspection (RI)** - a post delivery inspection performed as part of the acceptance process to verify that ordering requirements have been met. Receiving Inspection consists of a verification of all criteria specified on the RICP. Verifications performed remotely by on-site facilities such as bench testing, material mechanical property testing, electrical characteristic verification, etc., are also considered to be part of the receiving inspection even though they are not performed by FSS Quality Services Section. Within this procedure, a distinction is made as to who performs this activity. When the receiving inspection is performed by the FSS Quality Services Section, it is referred to as "R.I." When the receiving inspection is performed in the field, it is referred to as "field inspection" or "field dedication." "R.I.," "field inspection," or "field dedication" may also be performed to upgrade an item that was purchased Level 3. [3.46]

**Receiving Inspection Criteria Package (RICP)** - a listing of the minimum acceptance and/or receiving inspection criteria that the Responsible Engineer has determined are required in order to provide a reasonable assurance that the Level 1 or Level 2 item received is the item that was ordered. RICPs may also be created to upgrade an item that was purchased Level 3. [3.46]

**Record Drawing** - a controlled drawing that is used to support grassroot (new) modifications or to reflect the as-installed configuration (see as-built). [2.30]

**Redline** - mark-up of engineering documents reflecting approved changes. The redline mark-up constitutes a record of change (until incorporation) and is part of the implementing organization design or work documents. [1.57]

**Reference ID** - an alternate number that identifies a site component on an area specific drawing or sketch or in an area specific satellite database. [1.30]

**Registered Professional Engineer (RPE)** - an engineer registered in



the State of South Carolina to provide professional engineering services as described in the South Carolina Code of Laws, Title 40, Chapter 22. [1.40]

**Regression Testing** – Selective testing of an item, system, or component to verify that modifications have not caused unintended effects and that the item, system, or component complies with its specified requirements. Refer to Manual 1Q, QAP 20-1. [5.40]

**Reliability** - a measure of the ability of a system or component to perform as required. [3.04]

**Replacement item** - a new item or an item that replaces an original or installed item. A replacement item is classified as an "alternate replacement" or a "like-for-like replacement." [3.46]

**Replacement Item Evaluation/Commercial Grade Dedication Package (RIE/CGD)** – one means to document the attributes and process by which a commercial grade item will be determined to be acceptable for use in safety class or safety significant applications. Other acceptable means are through the use of a Receipt Inspection Criteria Package (RICP), Work Package (W/P) instructions, or some combination of the RICP, W/P instructions, and RIE/CGD. [3.46]

**Requirements Specification for Software (RSS)** – the controlling document for specifying the requirements of a software product. [5.10]

**Requirements Traceability Matrix (RTM)** – a document that traces requirements from the Requirements Specification for Software (RSS) to design elements in the DDS and to the completed testing documentation. [5.20]

**Risk Factor (RF)** - see [WSRC-IM-98-00033](#), Appendix B.

**Risk Handling** – see [WSRC-IM-98-00033](#), Appendix B.

**Risk Level** – see [WSRC-IM-98-00033](#), Appendix B.

**SSC Category** - grouping or combining SSCs having similar materials, service conditions, environmental conditions, and degradation history and tendencies. [3.48]

**SSC Examination Plan** - summary tables of SSCs subject to

examination or test and their required examination and test frequencies. [3.48]

**Safe Mission Essential** – the practice of specifying requirements, design attributes, and operating strategies that result in safe and successful DOE mission accomplishment at minimum life-cycle cost. [1.02]

**Safety Analysis** - see WSRC Manual 11Q, Facility Safety Document Manual. [2.25]

**Safety Analysis Report for Packaging (SARP)** - See WSRC Manual 19Q, Transportation Safety [4.05]

**Safety Basis (SB)** – See WSRC Manual 11Q, Facility Safety Document Manual.

**Safety Basis Strategy (SBS)** – a planned safety analysis approach for a proposed modification that is developed in accordance with procedure 1.10, Manual 11Q. [2.05]

**Safety Class** - the functional and safety classification that applies to those structures, systems, or components or Administrative Controls whose preventative or mitigative function is necessary to keep hazardous material exposure to the public below the Offsite Evaluation Guidelines. [2.25]

**Safety Class Function** - a preventative or mitigative function that must be performed to keep radiological exposure to the Public from challenging the Offsite Evaluation Guidelines. [2.25]

**Safety Class SSC** – an SSC that performs a Safety Class function. [2.25]

**Safety (SC/SS) Component** - a plant component or part thereof, necessary to assure the nuclear safety requirements of Manual E7, 2.25 are met for SSC(s) functionally classified as safety class or safety significant. [3.46]

**Safety SSCs** - the set of Safety Class and Safety Significant structures, systems, and components for a given facility. [2.25]

**Safety Significant** - the functional and safety classification that applies to those structures, systems, and components or

Administrative controls not designated as safety class SSCs but whose preventive or mitigative function is a major contributor to defense in depth (i.e., prevention of uncontrolled material releases) and/or worker safety as determined from hazard analysis. [2.25]

**Safety Significant Function** – a preventive or mitigative function whose performance is a major contributor to Defense in Depth (i.e., prevention of uncontrolled material releases) and/or Worker safety as determined from Hazard Analysis. [2.25]

**Safety Significant SSC** – an SSC that performs a Safety Significant Function. [2.25]

**Separation Group** - a field in the component number containing a single alpha character code (e.g., "A", "B", "C", etc.) and used to ensure that electrical cable will be routed in separate raceways for voltage, fire protection, or other reasons when redundant or backup circuits are required. [1.30]

**Service Level** - a field in the component number containing a single alpha character that designates the highest voltage level for the raceway systems, cables and jumpers. [1.30]

**Site Unit Area Clarifier** – a site area designator or an expression used to differentiate two or more items or functional operations that perform identical or similar functions. [1.30]

**Software** - Computer programs (including supporting operating systems, compilers, etc.), procedures, rules, associated documentation and data pertaining to the operation of a computer system. [5.61]

**Software Configuration Management (SCM)** – a discipline applying technical and administrative direction to identify and document the functional and physical characteristics of software configuration items, control modifications to the characteristics, record and report change processing and implementation status, and verify compliance with specified requirements. [5.62]

**Software Configuration Status Accounting (SCSA)** – the process of recording and reporting the status of approved computer programs, software technical documents, proposed modifications, and implementation of approved modifications. [5.62]

**Software Error Notification (SEN)** - The document used to notify appropriate persons of software errors. [5.61]

**Software Evaluation Package (SEP)** – A set of documents that is utilized to demonstrate adequate confidence that the existing or acquired software is acceptable for its intended end use. [5.07]

**Software Inventory Database** - Electronic and/or paper records that contain the configuration management and action tracking information required by this procedure for the Software Library management. [5.61]

**Software Library** - A controlled collection of software for distribution. [5.61]

**Software Modification** – the development and procurement of software as well as changes to configuration controlled software. [5.01]

**Software Modification Package (SMP)** – a Computer Program Modification Tracker and supporting documents. [5.62]

**Software Owner** - the individual accountable for all technical, administrative, and financial aspects of software or programmable devices. [2.31]

**Software Problem** - An anomaly that may produce a software error. Once an anomaly or problem is detected, an analysis is performed to determine if the anomaly is or has produced/resulted in an actual error. [5.61]

**Software Project Management Plan** - the document for controlling software project management activities by defining the administrative processes to develop the software products prior to final acceptance of the product by the Software Owner. [5.04]

**Software Provider** - Developer or vendor of a computer program. [5.61]

**Software Quality Assurance Plan (SQAP)** – the governing document for the software engineering process, including development, acquisition, configuration management and verification activities. [5.03]

**Software Test Case** – A specific set of test data and associated inputs, execution conditions, and expected results that determine whether the software being tested meets functional requirements. [5.40]

**Software Test Plan (STP)/Test Document** – A document or collection of documents for executing, controlling, and documenting the software testing process. [5.40]

**Software Tools** –computer programs used in the development, testing, analysis, or maintenance of a program or its documentation (e.g., assemblers, comparators, cross-reference generators, compilers, computer-aided software engineering tools, configuration and code management software, decompilers, disassemblers, editors, flowcharters, monitor test case generators, and timing analyzers.) [5.03]

**Source Verification (Verification Method 3)** - activities witnessed at the supplier's facilities by WSRC or its agent for specific items to verify that a supplier of a commercial grade item controls the critical characteristics of that item, as a method to accept the item. [3.46]

**Special Conditions and Requirements** - attributes beyond supplier normal parameters (e.g. seismic, environmental, operational requirements) required to satisfy authorization basis and operational requirements. [3.46]

**Special Tests and Inspections (Verification Method 1)** - activities conducted after receipt of a commercial grade item to verify one or more critical characteristics as a method to accept the item for safety use. [3.46]

**Specification** – a technical document used to provide a detailed description of requirements for items and/or services including installation. [2.14]

**SRP Drawing** - a drawing that was created prior to April 1989 and has not been revised to meet the requirements of this procedure. [2.30]

**Statistical Methodology** – Method used to perform accident analyses consequence calculations whereby distributions expressing the uncertainty in inputs are combined using Monte Carlo or similar

mathematical techniques to calculate a result. This method differs from many traditional methods that use values combined directly together to calculate a result. [2.25]

**Strong-Tight container** - See WSRC Manual 19Q, Transportation Safety [3.15]

**Structural Integrity** - the demonstrated capability of an SSC to perform its intended design functions under all operational and design basis events. [3.48]

**Structural Integrity Baseline** - measurements and analyses that establish the status, configuration, setting, or condition of an item. The structural integrity baseline of an item may be established prior to it being placed into initial operation, while it is in service, or after repair or replacement activities. [3.48]

**Structural Integrity Program** - periodic measurements (examinations, tests, observations) and analyses performed on structures, systems, and components to detect degradation and/or analyze its effect(s) on facility performance, safety, or reliability. [3.48]

**Structural Margins** - a measure of a component or its support to perform its design function safely, considering material properties, installed loadings, and operating and environmental conditions. [3.48]

**Structure, System, or Component (SSC)** - structures, systems (hardware and software), or components that have a boundary and are replaceable. SSCs are either configuration controlled or non-configuration controlled. [1.05]

**Supplemental Requirements** – additional supplier requirements or provisions (over and above normal for functional, technical and procurement quality requirements) for an SSC derived through evaluation of potential risk factors associated with the procurement and usage of the SSC. [3.10]

**Supplier** - any individual or organization who furnishes items or services in accordance with a procurement document. All-inclusive term used in place of the following: vendor, seller, contractor, subcontractor, dealer, fabricator, consultant, manufacturer,

distributor, and their sub-tier levels. [1.20]

**Support Document** - document types, in addition to Essential, that provide engineering, maintenance and operations the details necessary for plant operations. Support document types typically include facility and system design descriptions, MEL, and drawings as defined in Procedure Manual E7, Procedure 1.05. [1.05]

**Sustainable Design (SD)** – the use of multiple design concepts, including Pollution Prevention (P2), Energy Efficiency (E2), and Affirmative Procurement (AP), to consider the impact(s) of an activity, project, or product's life cycle on the sustainable use of environmental and energy sources. [1.41]

**System** - a collection of independent components integrated to perform a specific function or functions. [1.30]

**System Design Description (SDD)** - the facility system technical document that defines the functions, performance, design, physical, testing, interface, operating, and maintenance requirements for a system and the associated components. The SDD provides the single source for communicating and controlling the system and component level requirements. [2.12]

**System Software** - software designed to enable the operation and maintenance of a computer system and its associated computer programs (e.g., Windows NT, VMS and Unix.) [5.03]

**Systems Engineering Management Plan** - a control tool, internal to and maintained by the Project Team, which details the strategy for implementation of a disciplined systems engineering process. [2.04]

**Systems Engineering Process** – a structured approach that clearly defines the mission or problem, manages system functions and requirements, identifies and manages risk, establishes bases to conduct informed decision making, and verifies that products and services meet customer needs. [2.04]

**Task (T) Drawing** - a drawing that is controlled entirely by the technical agency for use in the design, procurement, construction, fabrication, installation or testing of Infrastructure and Industrial Modifications. [1.53]

**Task Requirements and Criteria Document (TR&C)** - a design

input document used to identify the purpose and need for a plant modification, to provide a general description of the objective(s) of the modification, to describe functional requirements with associated bases, to identify the alternatives evaluated and to establish the applicable design criteria at the appropriate level of detail necessary to proceed with the design of a plant modification. [2.13]

**Task Sponsor** - the custodian of the facility to be modified. [2.05]

**Technical Agency** - an organization designated by the Modification Manager to perform activities required for a software modification or to develop technical baseline documents in support of a plant modification. The Design Authority or Design Agency may serve as the Technical Agency for one or more of the modification activities. [2.05]

**Technical Assistance Request** - a document that requests technical work or information from a Technical Agency when the assistance is not expected to impact a technical baseline. [3.12]

**Technical Baseline** - all documents, including all safety documentation, used to identify, justify and demonstrate the physical, functional or operational requirements of configuration controlled structures, systems and components. [1.10]

**Technical Baseline List (TBL)** - a document that identifies the technical baseline documents for a facility grouped by system. [1.05]

**Technical Baseline Modification** - the development of a technical baseline for a new configuration controlled SSC or a change to the data in the technical baseline of an existing configuration controlled SSC. [1.05]

**Technical Baseline Task** - the technical work required to generate and document any of the activities of the technical baseline modification process. [2.02]

**Technical Errors** – mistakes or use of data that cause incorrect results

**Technical Evaluation** - an evaluation performed to assure that the correct technical requirements for an item are specified in the commercial grade documentation . [3.46]



**Technical Report** - a report or compilation of documentation that presents scientific facts or the results of technical work conducted by a Technical Agency in support of an operating or proposed facility. Technical reports in the context of this procedure include any documentation that supports decisions relating to the establishment or modification of a technical baseline. [3.60]

**Technical Risk** - any technical factor, element, constraint, or course of action that introduces as uncertainty of outcome or the possibility of deficiencies, inadequate performance, schedule delays or cost overruns. [2.05]

**Technical Risk Analysis** - an identification and evaluation process to determine if technical risks exist or would be created during the execution of a plant modification.[2.05]

**Technical Safety Basis Document**– a technical safety evaluation document consistent with the commensurate associated hazard (e.g., Safety Analysis Report for Packaging, Onsite Safety Assessment, Type A package approval documentation, Industrial package documentation, or Strong-Tight container documentation) [3.15]

**Technical Task Request (TTR)** - a documented request for technical services or information related to the validity of, or changes to, a technical baseline that usually requires support from Projects Engineering and Construction Division (PE&CD) or Savannah River Technology Center (SRTC). [2.02]

**Technology Assessment** - an evaluation of the ability of existing technology to implement a proposed plant modification. [2.07]

**Technology Development** - the development of new or unproven technologies; the application of existing technologies to new/different uses; or the combining of existing or proven technologies to achieve a specific goal. [2.07]

**Technology Development Program Plan** – a comprehensive planning document describing technology development activities required for the successful execution of an identified modification and their relationship to the overall modification scope and schedule. This may be referred to as a Technology or Research & Development (R&D) Roadmap. [2.07]

**Technology Review** – an independent assessment of the Technology Development activities for technical maturity and readiness to proceed to the next design phase of a proposed plant modification with acceptable risk. [2.61]

**Technology Review Committee** - the selected group of individuals that shall review and comment on the Data Package submitted for Technology Review. [2.61]

**Technology Review Data Package (Data Package)** - Technology Review information that includes the approved task input documents and task output documents and any supporting laboratory or pilot-facility analytical and test results for a plant modification under review. [2.61]

**Technology Review Report** - documentation prepared by the Technology Review Committee Chairperson presenting results from the Technology Review. Contains specific recommendations for path forward. [2.61]

**Temporary Modification** - modifications made to configuration controlled structures, systems, or components when the changes are not intended to be permanent and associated changes to the affected controlled documents are not incorporated. These modifications are temporary in that they are intended to be installed for six months or less, except for those required to establish an interface between an operating system and one in lay-up or otherwise support a lay-up. [2.06]

**Test Acceptance Criteria (TAC)** - a "critical" pre-defined qualitative or quantitative measurement that requires testing to satisfy a performance requirement(s). A "critical" measurement is one that is specified in the Safety Basis, involved in the protection of SS/SC systems, or specified in operating/licensing permits. [2.26]

**Tie-In** – connection of new or modified equipment to existing facilities. [3.80]

**Total Effective Dose Equivalent (TEDE)** – the sum of the deep dose equivalent (for external exposures) and the committed effective dose equivalent (for internal exposure). [2.25]

**Trend Analysis** - a systematic evaluation of monitored parameters to

identify and predict changes in the performance of a system or component. [3.04]

**Type 1 Calculation/Commercial Calculation** - an engineering calculation that is intended to be issued and controlled as an independent document (i.e. a stand-alone document). A type 1 calculation is statused as one of the following: [2.31 & 1.54]

- Preliminary Calculation – calculations made for estimates of performance, costs or scale which are not performed with the intent of being directly incorporated in final design documents. They may include calculations to be incorporated in cost studies, or bid specifications, or as estimates in reports to regulatory agencies.

Preliminary calculations may form the basis for preliminary safety analysis or preliminary design work, or for issue of drawings or specifications for construction or procurement when only preliminary data is available (e.g., data supplied on similar equipment manufactured for other modifications, designer's or supplier's knowledge of similar systems, etc). Such calculations will be revised to assume the status of confirmed calculations when confirmed data is available. Design and analysis work performed based on preliminary calculations shall be reviewed and revised as necessary if the results of confirmed calculations differ from the preliminary results.

- Confirmed Calculation – calculations that form the basis for preliminary safety analysis, drawings, specifications, or other design or safety analysis documents that are used to construct or operate the facility, or provide the design basis DSA for an operating facility, or for modifications to an operating facility. These calculations may be revised due to changes in design criteria, methods or other reasons. [2.31]
- Open Item – input that is not fully confirmed, or ongoing work related to the calculation, that is judged to:
  1. be essential to the conclusions of the calculations and,
  2. involve a high degree or amount of uncertainty such that eventual confirmation of the input or successful completion of the ongoing work is in doubt.

**Type 2 Calculation** - an engineering calculation intended for incorporation in, and to be approved as part of, other documentation

(i.e. not meant to be stand-alone). [2.31]

**Type 2 Commercial Calculation** - a commercial engineering calculation intended for incorporation in, and to be approved as part of, other documentation such as Field Change Requests and Non-Conformance Reports. (i.e., not meant to be stand-alone). [1.54]

**Type 2 Independent Review (IR-2)** – An independent review conducted by an individual subject to a different technical direction (i.e., not assigned to the same project or task). [5.03]

**Type B Quantity** – a quantity of radioactive material, for which the aggregate radioactivity exceeds A1 for special form or A2 for normal form. A1 and A2 values are given in Table A-1 at the end of 10 CFR 71 [4.05]

**USQ Qualified Individual** - an individual who has completed site-level training in the USQ program and facility-based training in the facility AB and has been designated by the Facility Manager as either a Screening Originator, Screening Reviewer, Evaluation Originator or Qualified Reviewer in accordance with Manual 11Q, Procedure 1.05. Such persons are authorized to determine if a modification will impact a DSA or other Safety Basis document per 11Q, 1.05. [2.05]

**Uniquely Tracked Commodity (UTC)** – A specific serialized physical item that is placed at a logical location (e.g., equipment or component) in a facility. [1.31]

**Unit** – a site area classifier or an expression used to differentiate two or more items or functional operations that perform identical or similar functions. [1.30]

**Unlikely** – frequency which is greater than or equal to 10-4 per year and less than 10-2 per year. [2.25]

**Unmitigated** - taking no credit for either preventors or mitigators. [2.25]

**Validation** – see WSRC Manual 1Q Glossary.

**Value System** - a set of specified criteria used to select the preferred alternative that exhibits the best level of performance to meet the functions and requirements consistent with any cost or schedule

considerations. [2.15]

**Vendor Technical Manual (VTM)** – a document that contains one or more vendor supplied technical documents for a specific group of components, as assembly, or a system. The terms Vendor Print File (VPF) or Blueprint File (BPF) may also be used. [2.30]

**Verification** – see WSRC Manual 1Q Glossary.

**Verification Method** – Methods used to verify technical and quality requirements and critical characteristics. Four methods may be used, either individually or in combination. They are:

- Method 1 – Special Tests and Inspections
- Method 2 – Commercial Grade Survey of Supplier
- Method 3 – Source Verification
- Method 4 – Acceptable Supplier/Item Performance Record [3.46]

**Walkdown** - a visual inspection of facility SSCs to identify the as-found physical configuration and any discrepancies with currently approved facility documentation. [1.05]

**Witness Point** - an inspection activity beyond which work shall not proceed until an inspector is notified and (1) the inspection is performed and released, or (2) the inspection is deferred and can be completed at a later time, or (3) the witnessing of the work activity by the inspector is waived by Engineering. [2.36]

**Work Authorization** - approval to process work control documents and proceed with physical modification prior to DCF approval. [2.37]

**Work Package** - A collection of documents used to authorize work, provide instructions for the work, and document accomplishment of the work. [3.46]

**Worker** - population within the site boundary. [2.25]

Unless otherwise noted, the Conduct of Engineering web page and subsequent pages do not contain Sensitive Unclassified Information (SUI).